THE NEIGHBOURHOOD OFFICE PRIVACY POLICY

Updated 20th March 2022

Version: 2

Welcome to The Neighbourhood Office's privacy policy ("the Policy").

At The Neighbourhood Office we respect your privacy and are committed to protecting your personal data. We wish to help you make informed decisions, so please take a few moments to read the sections below and learn how we may use your personal information.

1. PURPOSE OF THIS POLICY

We have provided this Policy to help you understand how we collect, use and protect your information when you use our services.

The purposes of this Policy are:

i. To protect the privacy of individuals whose personal information is collected or used by the Neighbourhood Office;
ii. To ensure that the Neighbourhood Office complies with relevant data protection law;
iii. To describe and promote best practice concerning data protection and data security; and
iv. To protect the Neighbourhood Office from the risks of a data protection breach.

2. SCOPE AND RESPONSIBILITIES

This Policy applies to:

i. personal information concerning users and members of the Neighbourhood Office;
ii. all Neighbourhood Office staff and contractors who handle such personal information.

The board of directors of the Neighbourhoodoffice Limited is ultimately responsible for ensuring that the Neighbourhood Office meets its legal obligations, with operational responsibility delegated to the Managing Director.

This Policy ensures that we comply with relevant Data Protection laws. It is based on the privacy framework in the UK and the EU including the EU General Data Protection Regulation ('GDPR').

We have appointed a data protection officer (DPO) who is responsible for overseeing questions in relation to this Policy. If you have any questions about this Policy, including any requests to exercise your legal rights, please contact the DPO using the details set out below.

Full name: Kerry Carmichael
Email address: kerry@theneighbourhoodoffice.com
Postal address: 40 Bermondsey Street, London, SE1 3UD
Telephone number: +44 777 260 9007

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues (www.ico.org.uk). We would, however, appreciate the chance to deal with your concerns before you approach the ICO so please contact us in the first instance.

3. CHANGES TO THE PRIVACY POLICY AND YOUR DUTY TO INFORM US OF CHANGES

We keep this Policy under regular review. We ensure as far as possible that the personal information we collect, and use is

accurate and up-to-date. This includes:

i. Ensuring that personal information communicated to us is recorded accurately;
ii. Taking appropriate steps to verify the accuracy of the personal information; and,
iii. Implementing measures for checking and rectifying data which appears to be inaccurate.

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

4. THE DATA WE COLLECT ABOUT YOU

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

We only collect and use personal information which is necessary for the purpose and take steps to avoid the unnecessary collection and use of personal information. This information is limited to:

- names and contact details of the Neighbourhood Office members;
- names and contact details of any guests of the Neighbourhood Office members;
- names and contact details of the director of each member company, as well as a copy the director's identification document;
- members' payment information.

We do not collect any Special Categories of Personal Data about you (this includes, for example, details about your race or ethnicity, religious or philosophical beliefs or sexual orientation).

5. IF YOU FAIL TO PROVIDE PERSONAL DATA

Where we need to collect personal data by law, or under the terms of the membership contract and you fail to provide that data when requested, we may not be able to perform the services. In this case, we may have to cancel a product or service you have with us but we will notify you if this is the case at the time.

6. HOW IS YOUR PERSONAL DATA COLLECTED AND HOW WE USE YOUR PERSONAL DATA

We collect your personal information by direct interactions. You give us your Personal Data by filling in forms or by corresponding with us by email or otherwise.

We will only use your personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances:

i. By managing the co-working office space;
ii. Through managing your co-working membership; and by
iii. Organising and promoting the Neighbourhood Office events at the premises.

7. DISCLOSURES OF YOUR PERSONAL DATA

We may share your personal data with the parties set out below for the purposes as described hereunder.

External Third Party	Purpose/Activity	Type of data	Lawful basis for processing
OfficeRnD Limited.	OfficeRnD is a software that manages our membership platform. For example, it creates address books of our members and respective	Name, surname, email address and telephone number.	Performance of a contract with you.

	companies, runs billing processes, and allows members to book meeting rooms. In addition, it is a visitor management software. As such, personal data is shared with Office RnD allowing it to notify members when their guests arrive to site. It also ensures that we can keep a record of all person who access the premises.		
Go Cardless Ltd	GoCardless process membership payments and other payment requirements.	Name, surname, email, address and telephone.	Performance of a contract with you. Necessary for our legitimate interests.
Xero Ltd.	Xero manage and provide all of our accounting solutions.	Name, surname, email, address and telephone.	Performance of a contract with you. Necessary for our legitimate interests.
ACT Access Software Ltd.	We use ACT Access Software to generate member access cards and manage member access rights.	Name, surname and email address.	Performance of a contract with you.

We require all third parties to respect the security of your personal data and to treat it in accordance with the law. We do not allow our third-party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions.

Where personal information is shared with other parties (apart from where this is under a legal obligation) this is governed by a data processing agreement which sets out the parties' obligations to keep the information secure and only to use it lawfully.

8. INTERNATIONAL TRANSFERS

Some of our external third parties are based outside the EEA so their processing of your personal data will involve a transfer of data outside the EEA.

Whenever we transfer your personal data out of the EEA, we ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

- We will only transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data by the European Commission.
- Where we use certain service providers, we may use specific contracts approved by the European Commission which give personal data the same protection it has in Europe.
- Where we use providers based in the US, we may transfer data to them if they are part of the Privacy Shield which requires them to provide similar protection to personal data shared between Europe and the US.

Please contact us if you want further information on the specific mechanism used by us when transferring your personal data out of the EEA.

9. DATA SECURITY

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties on a need to know basis. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

Our technical and organisational measures include the following:

i. We do not maintain any servers on site. All personal information is stored on secure hosted platforms.
ii. Our staff are only given access to electronic filing systems and folders to the extent that this is necessary to enable each staff member to fulfil his or her duties.
iii. Access to hosted data systems is password-protected.
iv. Staff use their own mobile phones for their business that are password protected.
v. Staff are required to log-off from systems and laptops when not in use.
vi. Staff are provided with training and guidance on the secure use of electronic devices in public and the associated risks.
vii. Staff are prohibited from disclosing passwords or writing them on post-it notes.
viii. We do not maintain any paper records containing personal information.
ix. We ensure that our physical premises are secure from theft and other intrusion.
x. The management of our IT systems is the delegated responsibility of a third-party provider. The Managing Director is responsible for ensuring that these services provide an appropriate level of security. Our IT systems are reviewed for data security compliance purposes at intervals of no more than 12 months.

10. PERSONAL DATA BREACH

A personal data breach is defined as 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data'. This might include, for example the loss of papers containing personal information or the loss of a laptop.

We are required to report any breach to the Information Commissioner's Office as soon as possible and in any event within 72 hours of becoming aware of a breach. This does not apply if the breach is unlikely to result in a risk to the rights and freedoms of individuals.

We maintain procedures for responding to a data protection breach. This comprises of:

i. An effective channel of communication to ensure that breaches can be reported, and that relevant staff are notified immediately, including out of hours reporting;
ii. A process for assessing the reported breach, considering whether it needs to be reported to the Information Commissioner's Office and to the individual or individuals concerned, assessing its seriousness and the likely damage and identifying steps to mitigate that damage;
iii. A process for reporting breaches to the Information Commissioner's Office and to the individual or individuals concerned; and,
iv. A process for evaluating the circumstances leading to the breach and, if required, implementing remedial measures such as further training or guidance.

11. DATA RETENTION

We retain personal information concerning members for the duration of your membership. Once the membership has expired information is retained for accounting and tax purposes for seven years and then securely deleted. Information which does not relate to accounting and tax records is securely deleted 30 days after notification of the membership being terminated.

We maintain a system for checking whether memberships are still active at intervals of no more than six months, closing inactive accounts and deleting information as stated above. Members are reminded at registration that the burden is on them to inform us when their membership ends.

We retain personal information about guests to avoid frequent visitors from having to re-register at every visit and to maintain security of the premises. This information is securely deleted at the expiration of six months after the guest's most recent visit to the site.

12. ACCOUNTABILITY AND GOVERNANCE

In addition to specific record keeping mentioned elsewhere in this Policy, we maintain the following:

i. An inventory of personal information and its collection and use;
ii. A record of data protection incidents; and
iii. A repository of all data protection policy documents, procedures and other guidance.

13. YOUR LEGAL RIGHTS

Under certain circumstances, you have rights under data protection laws in relation to your personal data, these include the following:

- Request access to your personal data.
- Request correction of your personal data.
- Request erasure of your personal data.
- Object to processing of your personal data.
- Request restriction of processing your personal data.
- Request transfer of your personal data.
- Right to withdraw consent.

If you wish to exercise any of the rights set out above, please contact us.

14. PRIVACY SUPPORT

We reserve the right to amend or modify this Policy at any time and in response to changes in applicable data protection and privacy legislation and to reflect changes in products or services.

If we decide to change our Policy, we will post the changes on our website and Online Membership Portal. If at any point we decide to use personal information in a manner different from that stated at the time it was collected, we will tell you. You will have a choice as to whether or not we are able to use your information in this different manner.

We may change the content of our website without notice Consequently, our Privacy Policy may be amended at any time in the future to reflect those changes, or changes in the applicable law. We therefore encourage you to review them from time to time to stay informed of how we are using personal information.

If you have any enquiry about our Policy or practices, please contact us.