

GENERAL PRIVACY NOTICE – WHITEHALL BID

INTRODUCTION

Welcome to the Whitehall Business Improvement District (“Whitehall BID”) privacy notice.

Whitehall BID is one of four BIDs (Victoria, Victoria Westminster, Whitehall and The Northbank) that make up London Heritage Quarter (“London HQ Limited”). All five companies are managed by the same Executive Team, and as such are joint controllers of personal data, and subject to a Data Sharing Agreement.

Whitehall BID respects and values your privacy and is committed to protecting your personal data under “Data Protection Legislation”. This privacy notice will inform you as to how we look after any personal data we collect from you or that you provide to us and tell you about your data protection rights and how the law protects you. This privacy notice applies to you if you are a visitor to our website or a levy payer. If you are an employee of London HQ then the relevant Privacy Notice can be found on Cezanne.

“Data Protection Legislation” means all applicable legislation in force from time to time in the United Kingdom applicable to data protection and privacy including, but not limited to, the UK GDPR (the retained EU law version of the General Data Protection Regulation ((EU) 2016/679), as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018); the Data Protection Act 2018 (and regulations made thereunder); and the Privacy and Electronic Communications Regulations 2003 as amended.

1. Important information and who we are

- 1.1. This privacy notice sets out the basis on which we will process any personal data we collect from you, or that you provide to us.
- 1.2. It is important that you read this privacy notice together with any other privacy notice or fair processing notice we may provide on specific occasions when we are collecting or processing personal data about you so that you are fully aware of how and why we are using your data. This privacy notice supplements the other notices and is not intended to override them. For the purpose of applicable data protection legislation, we are the data controller of the data that you provide to us.
- 1.3. Whitehall BID is the controller and responsible for your personal data (referred to as "we", "us" or "our" in this privacy notice).
- 1.4. We have appointed a Data Protection Manager who is responsible for overseeing questions in relation to this privacy notice. If you have any questions about this privacy notice, including any requests to exercise your legal rights, please contact the Data Protection Manager using the details set out below.
- 1.5. Our full details are:

Full name of legal entity:	Whitehall BID Limited
ICO Registration Number:	ZB343061
Name or title of Data Protection Manager:	Katherine Fleming
Email address:	info@london-hq.co.uk (Subject: Governance)
Postal address:	54 Wilton Road, London SW1V 1DE
Telephone number:	020 3004 0794

2. Complaints

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 notice and your duty to inform us of changes

It is 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. Third-party links

This website may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements. When you leave our website, we encourage you to read the privacy notice of every website you visit.

5. The data we collect about you

- 5.1. 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).
- 5.2. The personal data we collect includes but is not limited to: name, email address, postal address, telephone number, the company you work for, job title, the industry you work in and bank account information/transaction details (the latter only for the purposes of paying invoices).
- 5.3. We also collect, use and share **Aggregated Data** such as statistical or demographic data for any purpose when you access our website. Aggregated Data may be derived from your personal data but is not considered personal data in law as this data does not directly or indirectly reveal your identity. For example, we may aggregate your Usage Data to calculate the percentage of users accessing a specific website feature. However, if we combine or connect Aggregated Data with your personal data so that it can directly or indirectly identify you, we treat the combined data as personal data which will be used in accordance with this privacy notice.
- 5.4. We collect and process data relating to those known or suspected to have committed anti-social behaviour and/or criminal offences within the BID area. This is for the purposes of reporting and preventing crime, fraud and anti-social behaviour. You can view our separate Privacy Notice for Offenders [here](#).
- 5.5. We collect and process data relating to vulnerable and at-risk persons within the BID area. This is to provide them with welfare support and prevent them coming to harm. You can view our separate Privacy Notice for Vulnerable Persons [here](#).

6. If you fail to provide personal data

- 6.1. Where we need to collect personal data by law, or under the terms of a contract we have with you or are trying to enter with you (for example, to provide you with goods or services) and you fail to provide that data when requested, we may not be able to perform the contract we have. 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.

7. How is your personal data collected?

We use different methods to collect data from and about you including through **Direct interactions** - you may give us your data corresponding with us by post, phone, email or otherwise. This includes personal data you provide when you:

- 7.1.1. apply for or make enquiries to us about our operations, projects or services
- 7.1.2. attend London HQ events
- 7.1.3. subscribe to our newsletter, privilege cards, emergency notifications or download, register and use our London HQ Hub Mobile App.
- 7.1.4. Providers of technical, payment and delivery services who during their work need to provide us with your contact, financial and transaction data.
- 7.1.5. Publicly available sources such as Companies House, websites and social media

platforms that hold your identity and contact data.

8. How we use your personal data

- 8.1. We will use your personal information:
 - 8.1.1. To register you and contact you after you have registered your interest with our organisation
 - 8.1.2. To provide you with services or information you have requested
 - 8.1.3. To contact you regarding projects and services that might be of interest to you and your organisation as members of one of the four BIDs that make up London HQ.
 - 8.1.4. To maintain our own accounts and records
 - 8.1.5. To ensure payment of any Business Improvement District Levy owed to us by your organisation.
 - 8.1.6. To facilitate voting by eligible businesses in any BID ballot process
 - 8.1.7. To obtain survey results or request feedback on our services

9. Our lawful basis for processing

- 9.1. 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:
 - 9.1.1. Where we need to perform the contract we are about to enter into or have entered into with you (Article 6(1)(b) UK GDPR).
 - 9.1.2. 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 (Article 6(1)(f) UK GDPR).
 - 9.1.3. Where we need to comply with a legal or regulatory obligation (Article 6(1)(c) UK GDPR).
- 9.2. Generally, we do not rely on consent as a lawful basis for processing your personal data other than in relation to sending direct marketing communications to you via email or text message. You have the right to withdraw consent to marketing at any time by contacting us.
- 9.3. Note that we may process your personal data for more than one lawful basis depending on the specific purpose for which we are using your data. Please contact us if you need details about the specific lawful basis we are relying on to process your personal data.
- 9.4. When we are processing special category data, such as the health data of vulnerable individuals living on the streets, we are doing so in the substantial public interest (Article 9.2.g UK GDPR) for the safeguarding of children and individuals at risk (in line with paragraph 18 of Schedule 1 of the DPA 2018).
- 9.5. When we are processing personal data in relation to the prevention and detection of crime, we are doing so under the terms of our Information Sharing Agreements with the Metropolitan Police, British Transport Police and Westminster City Council.

10. Marketing

- 10.1. We strive to provide you with choices regarding certain personal data uses, particularly around marketing and advertising. We have established the following personal data control mechanisms.
- 10.2. We may use your Identity, Contact, Technical, Usage and Profile Data to form a view on what we think you may want or need, or what may be of interest to you. This is how we decide which products, services and offers may be relevant for you (we call this marketing). You will receive marketing communications from us if you have registered online for our newsletters or otherwise requested that you are added to the mailing list for them.
- 10.3. Opting out - you can ask us to stop sending you marketing messages at any time by following the opt-out links on any marketing message sent to you or by contacting us at any time.
- 10.4. Cookies - you can set your browser to refuse all or some browser cookies, or to alert you when websites set or access cookies. If you disable or refuse cookies, please note that some parts of this website may become inaccessible or not function properly. For more information about the cookies we use, please contact us to request our cookies policy.
- 10.5. Change of purpose - we will only use your personal data 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 you wish to get an explanation as to

how the processing for the new purpose is compatible with the original purpose, please contact us.

If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the lawful basis which allows us to do so.

Please note that we may process your personal data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

11. Disclosures of your personal data

- 11.1. We only disclose your personal data to third parties for the purposes set out in paragraph 8. We require all third parties to respect the security of your personal data, to treat it in accordance with the law and only process it in accordance with our instructions.
- 11.2. Internal third parties are The Northbank, Victoria and Victoria Westminster Business Improvement Districts and London HQ Limited due to fact that these are managed by the same executive team.
- 11.3. External third parties are:
 - Eventbrite – when we are organising events
 - Mailchimp – to provide you with email communications
 - Survey monkey - when we are conducting surveys
 - Vicinity - LHQ Hub App Agency
 - Yudu – a digital publishing software platform who host Sentinel
 - Westminster City Council
 - The Welcome People (providers of our Ambassador & Security Team)
 - Approved consultants appointed on a project-by-project basis
- 11.4. Third parties to whom we may choose to sell, transfer, or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. If a change happens to our business, then the new owners may use your personal data in the same way as set out in this privacy notice.

12. International transfers

- 12.1. We transfer your personal data outside the UK and European Economic Area (EEA) as some of our data is hosted on servers in the USA, so the processing of data by these external third parties will involve a transfer of data outside the EEA.
- 12.2. Whenever we transfer your personal data out of the EEA to the USA, we do so under the UK-US “Data Bridge” which is an extension to the EU-US Data Privacy Framework (DPF) adopted in July 2023. This enables organisations in the UK to transfer personal data to organisations in the USA that have certified to the DPF.
- 12.3. 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. For further details, see European Commission: Adequacy of the protection of personal data in non-EU countries.
- 12.4. Please contact us if you want further information on the specific mechanism used by us when transferring your personal data out of the UK and EEA.

13. Data security

- 13.1. We have put in place appropriate security measures (encrypted storage and access controls) 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 who have a business need to know. They will only process your personal data on our instructions and will do so in accordance with all relevant data protection legislation.
- 13.2. We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

14. Data retention

- 14.1. We will only retain your personal data 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.
- 14.2. 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 unauthorized use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.
 - 14.3. Details of retention periods for different aspects of your personal data are available on request by contacting us.
 - 14.4. In some circumstances you can ask us to delete your data: see “Request erasure” below for further information.
 - 14.5. In some circumstances we may anonymize your personal data (so that it can no longer be associated with you) for research or statistical purposes in which case we may use this information indefinitely without further notice to you.

15. Your legal rights

- 15.1. Under certain circumstances, you have rights under data protection legislation in relation to your personal data.
 - 15.1.1. Request access to your personal data (commonly known as a ‘data subject access request’). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.
 - 15.1.2. Request correction of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.
 - 15.1.3. Request erasure of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.
 - 15.1.4. Object to processing of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.
 - 15.1.5. Request restriction of processing of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios: (a) if you want us to establish the data’s accuracy; (b) where our use of the data is unlawful but you do not want us to erase it; (c) where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or (d) you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.
 - 15.1.6. Request the transfer of your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.
 - 15.1.7. Withdraw consent at any time where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.
- 15.2. If you wish to exercise any of the rights set out above, please contact us at info@london-hq.co.uk (subject: Governance) or in writing at the office address at the beginning of this policy document.

- 15.3 You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances.
- 15.4 We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.
- 15.4 We try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

16. Glossary

- 16.1. Lawful Basis
 - 16.1.1. “Legitimate Interest” means the interest of our business in conducting and managing our business to enable us to give you the best service/product and the best and most secure experience. We make sure we consider and balance any potential impact on you (both positive and negative) and your rights before we process your personal data for our legitimate interests. We do not use your personal data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law). You can obtain further information about how we assess our legitimate interests against any potential impact on you in respect of specific activities by contacting us.
 - 16.1.2. “Performance of Contract” means processing your data where it is necessary for the performance of a contract to which you are a party or to take steps at your request before entering such a contract.
 - 16.1.3. “Comply with a legal or regulatory obligation” means processing your personal data where it is necessary for compliance with a legal or regulatory obligation that we are subject to.