



CANARY WHARF GROUP PLC

General Privacy Notice

1. Introduction

Canary Wharf Group plc and its group companies ("Canary Wharf Group", "we", "us") of One Canada Square, Canary Wharf, London E14 5AB is the data controller of your personal data described in this notice. We respect the privacy of individuals and this notice explains what personal data we collect, why, on what legal bases, who we share it with, how long we keep it and the rights you have.

This notice applies when you visit the Canary Wharf estate (including by vehicle), use our websites or apps, contact or transact with us, attend our events, apply for a job with us, or are assisted by or otherwise come to the attention of our security personnel. Employees and contractors should also refer to our Privacy Notice for Employees and Contractors, and job applicants to our Privacy Notice for Candidates.

You can contact our Data Protection Officer at dataprotection@cwg.com or by writing to Data Protection, Canary Wharf Group, One Canada Square, Canary Wharf, London E14 5AB.

2. The personal data we collect

Most of the information we hold is provided by you directly, captured by our estate systems when you visit, or observed through your use of our websites. The main categories are:

- Contact and identity details: name, title, date of birth, postal address, telephone numbers and email addresses.
- Estate security data: CCTV images; video and audio recorded by body-worn cameras used by our security officers; recordings of security radio communications; incident reports, security officers' notebook entries and statements, and incident reports submitted to us by businesses on the estate; visitor, access and accident logs; and records of banning notices, warnings and related images (see section 3).
- Vehicle data: vehicle registration number, time and location of entry and exit, and associated images, collected by Automatic Number Plate Recognition (ANPR) cameras at estate entry and exit points.
- Business relationship information: your industry, job title, contacts and records of interactions with us, and financial and payment details where we contract with you or you supply us.
- Website and app data: information gathered via cookies and analytics, recordings of telephone calls to us, and any content or images you choose to upload to an account or profile (which you may change or remove, and for which you are responsible).

- Information you give us when applying for a job, registering for information, responding to consultations or contacting us for any other reason.
- Special category data in limited cases: information about your health, race or ethnicity where you provide it so we can support you at our sites or events, for equal-opportunities monitoring, or where it is recorded in connection with an accident or security incident.

3. CCTV, body-worn cameras and estate security

The Canary Wharf estate is monitored by CCTV, and our security officers may activate body-worn cameras, which record video and audio, when dealing with incidents. Radio communications between security officers and our Estate Control Centre are also recorded. Signage on the estate indicates where recording takes place. This data is processed to keep the estate, its occupiers and visitors safe; to prevent and detect crime and anti-social behaviour; to manage, investigate and record incidents and accidents; and to respond to complaints and legal claims.

If you are involved in a security incident, we may create an incident record which can include footage, audio, officers' statements, reports made to us by businesses on the estate, and information about the outcome. Where a banning notice or warning is issued to you, we keep a record of it, and your image may be circulated to our security personnel for the duration of the notice so that it can be applied. We review such records, and remove or correct them, where the information underlying them proves inaccurate or the measure is no longer justified.

Recordings of incidents may be reviewed internally for incident management, audit and quality purposes, and may be shared, under strict confidentiality and deletion obligations, with external professional advisers and security training specialists so that the handling of an incident (including any use of force by our officers) can be independently assessed and lessons applied. Footage and incident information may also be shared with the police and other law enforcement agencies, including through secure evidence-sharing platforms, where they request it for the prevention, detection, investigation or prosecution of crime.

Some security records relate to actual or suspected criminal offences. We process criminal offence data only as permitted by Article 10 UK GDPR and Schedule 1 to the Data Protection Act 2018, including where it is necessary for the prevention or detection of unlawful acts or in connection with legal claims.

4. How we use your personal data and our lawful bases

We use your personal data to: ensure site safety, security and operational integrity; prevent and detect crime, anti-social behaviour and unauthorised access; manage, investigate and record incidents, accidents, complaints and claims; provide goods, services, facilities and events you request; respond to your enquiries and consultations; process job applications; operate, secure and improve our websites and apps; meet our reporting, budgeting, audit, insurance and regulatory obligations; and, with your consent where required, send you marketing and use

recordings or images of you for promotional purposes.

Our lawful bases are: performance of a contract with you (goods, services, supplier and tenancy relationships); compliance with our legal obligations (for example, health and safety, financial reporting and responses to lawful requests from authorities); our legitimate interests (running a safe and secure estate, protecting people and property, investigating and responding to incidents, complaints and claims, pursuing our business interests, improving our services and training our personnel), where those interests are not overridden by your rights; and your consent, where we rely on it (for example, for marketing or promotional filming), which you may withdraw at any time. Where we process special category data we rely on an applicable condition under Article 9 UK GDPR and the Data Protection Act 2018, such as your explicit consent, protection of vital interests, or the establishment, exercise or defence of legal claims.

5. Who we share your personal data with

Your personal data is accessed by our employees on a need-to-know basis. We may also share it with:

- contractors, suppliers, professional advisers, insurers and service providers who perform functions on our behalf under contract, including providers of our security, incident management and evidence-sharing systems;
- external professional advisers and security training specialists engaged to review the handling of security incidents, as described in section 3;
- the police, law enforcement agencies, local authorities and regulators, where they may lawfully request information for the prevention and detection of crime, the apprehension or prosecution of offenders, or the assessment or collection of tax, or where we are otherwise required or permitted by law to provide it;
- businesses on the Canary Wharf estate, where we have a legitimate interest or other lawful basis to share it, for example to prevent or detect unlawful acts or to protect the public;
- our joint venture and business partners, where we reasonably believe a product or event is of interest to you and it is appropriate to share your business contact details; and
- other users of the Canary Wharf App, in respect of content you choose to share publicly via your profile.

The Canary Wharf Business Crime Reduction Partnership (BCRP): if you are suspected of committing an offence or anti-social behaviour on the estate, your personal data may be shared under the BCRP scheme, through which local businesses, the police and local authorities share information to prevent, detect and reduce crime and anti-social behaviour. The Canary Wharf BCRP privacy notice, available on our website and those of other scheme members, explains this in more detail.

6. Security and international transfers

We take appropriate technical and organisational measures to keep your personal data secure and to protect it against misuse, loss and unauthorised access, and our contracts with third parties require them to do the same. If your personal data is transferred outside the UK or the European Economic Area (the EU member states plus Norway, Iceland and Liechtenstein), we will only do so where the transfer complies with applicable data protection law and adequate safeguards are in place. Where you use services provided by third parties, such as the Canary Wharf visitor or resident apps, please also read those providers' own privacy notices.

7. How long we keep your personal data

We keep personal data only for as long as necessary for the purposes for which it was collected, taking account of legal minimum retention requirements. Indicative periods:

- CCTV footage: 28 days, then deleted automatically, unless preserved for an incident, investigation, request or claim;
- body-worn camera recordings: 28 days, on the same basis;
- recordings of security radio communications: 28 days, on the same basis;
- footage and recordings linked to a logged incident: retained for as long as the incident, any complaint, request or claim remains open;
- incident management records: 5 years;
- banning notice records and associated images: the duration of the notice, after which circulated images are withdrawn;
- ANPR data: 28 days, unless required for an investigation or legal purposes or retained in anonymised, aggregated form for traffic management;
- visitor pass data: 39 months following pass or QR code deactivation; and
- financial and statutory records: 7 years.

Where data is the subject of an information rights request, complaint, investigation or actual or anticipated legal claim, it is preserved for as long as that matter requires but records of the request itself and any response will be retained for held . Contact dataprotection@cwg.com for further information about retention.

8. Your rights

You have the right to: access your personal data and receive the supplementary information described in Article 15 UK GDPR; have inaccurate data corrected and incomplete data completed; have your data erased in certain circumstances; restrict processing in certain circumstances; object to processing based on our legitimate interests; data portability in respect of data you provided to us that we process by automated means on the basis of consent or contract; and withdraw any consent at any time, without affecting processing already carried out.

To exercise any right, contact us in writing using the details in section 11. We may need to verify your identity. We will respond within one month of receiving your request (or of verifying your identity, if later); where a request is complex or we receive a number of requests from you, we may extend this by up to two further months, and we will tell you within the first month if so. Exercising your rights is free of charge; where a request is manifestly unfounded or excessive, we may charge a reasonable fee or refuse to act on it, and we will explain why.

9. Automated decision-making

We do not make decisions about you based solely on automated processing, including profiling, which produce legal effects concerning you or similarly significantly affect you. ANPR and CCTV systems capture data automatically, but decisions arising from that data (for example, about access or incidents) involve human review.

10. Cookies and changes to this notice

Our websites use cookies to enhance your browsing experience; details are in the Cookies Policy on our websites. This notice may change as our business changes; the effective date appears at the end, and material changes will be highlighted on our website.

11. Contact, complaints and the ICO

If you have any questions about this notice or how we handle your personal data, or you are not satisfied, please contact us first so that we can resolve your concerns:

dataprotection@cwg.com, or Data Protection, Canary Wharf Group, One Canada Square, Canary Wharf, London E14 5AB.

If you wish to make a data protection complaint, you may use our Data Protection Complaints Form, available from dataprotection@cwg.com. We will acknowledge your complaint within 5 working days and respond within 30 days.

You also have the right to lodge a complaint with the Information Commissioner's Office at any time: www.ico.org.uk/concerns, 0303 123 1113, or Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

Effective Date: September 2026