CANARY WHARF
GROUP PLC

DATA PROTECTION POLICY

Contents

Paragraph **Page**

PART ONE: DATA PROTECTION

1 Principles

1.1. During the course of our activities Canary Wharf Group plc and all associated group companies ("**Canary Wharf Group**") will collect, store and process personal data about our clients, customers, suppliers and other individuals with whom we communicate. We recognise that the fair, transparent and lawful treatment of this data will maintain confidence in our organisation.

1.2. Data users and data processors must comply with, and behave in manner that facilitates our compliance with, this policy when processing personal data on our behalf. Any breach of this policy by our employees may result in disciplinary action.

1.3. We will ensure that personal data is:

1.3.1. Processed lawfully, fairly and in a transparent manner in relation to individuals.

1.3.2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

1.3.3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

1.3.4. Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

1.3.5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures in order to safeguard the rights and freedoms of individuals.

1.3.6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

1.4. We will demonstrate compliance with the principles listed above.

1.5. To comply with data protection laws and the accountability and transparency obligations, we will demonstrate our compliance by meeting the following data protection obligations:

1.5.1. Fully implement all appropriate technical and organisational measures

1.5.2. Maintain up to date and relevant documentation on all processing activities

1.5.3. Conducting Data Protection Impact Assessments

1.5.4. Implement measures to ensure privacy by design and default, including:

1.5.4.1. Data minimisation

1.5.4.2. Pseudonymisation

1.5.4.3. Transparency

1.5.5. Allowing individuals to monitor processing

1.5.6. Creating and improving security and enhanced privacy procedures on an on-going basis

1.6. Information about what data we collect and how it is used will be set out in a Privacy Notice issued to all data subjects and made available on our website.

2 Definition of Data Protection Terms

2.1. **Data subjects**, for the purpose of this policy, include all living individuals about whom we hold personal data.

2.2. **Personal data** means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2.3. **Data controller** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal

data. We are the data controller of all personal data used in our business for our own commercial purposes.

2.4. **Data users** are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

2.5. **Data processor** means a natural or legal person, public authority, agency or other body which processes personal data on our behalf and on our instructions and which is not a data user.

2.6. **Processing** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

2.7. **Sensitive personal data** is a special category of personal data, including information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health, sex life or sexual orientation, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

3 Fair and Lawful Processing

3.1. For personal data to be processed lawfully, one of the following legal grounds must apply. We shall only process personal data if:

3.1.1. the data subject has consented to processing;

3.1.2. processing is necessary in order to perform a contract with the data subject;

3.1.3. processing is necessary to comply with a legal obligation to which we are subject;

3.1.4. processing is necessary to protect the vital interests of the data subject or of another natural person;

3.1.5. processing is necessary for the performance of a task carried out in the public interest; or

3.1.6. processing is necessary for the purposes of the legitimate interest of the data controller or the party to whom the data is disclosed (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject).

3.2. When sensitive personal data is being processed, additional conditions must be met, including receiving explicit consent from the data subject and we shall ensure that such conditions are met when we are processing personal data as data controllers in the course of our business.

3.3. Whenever we collect personal data, it must be for a specific and legitimate purpose, which shall be notified to the data subject. We shall not further process data in a manner which is incompatible with the purpose or purposes for which it was collected.

3.4. We shall ensure that personal data we hold is accurate and kept up to date. We shall check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We shall take all reasonable steps to destroy or amend inaccurate or out-of-date data.

3.5. We shall not keep personal data longer than is necessary for the purpose or purposes for which it was collected. We shall take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

3.6. We shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation in an effective manner and integrate the necessary safeguards into the processing in order to meet the requirements of the law and protect the rights of data subjects.

4 Notifying Data Subjects[1]

4.1. Where we collect personal data directly from data subjects, we shall inform the data subject of:

4.1.1. the purpose or purposes and legal basis for which we intend to process that personal data;

4.1.2. if applicable, the legitimate interest pursued in accordance with paragraph 3.1.6;

[1] Please see our Privacy Notice

4.1.3. the types of third parties, if any, with which we will share or to which we will disclose that personal data;

4.1.4. if applicable, the fact that we intend to transfer such personal data overseas, together with a reference to the applicable safeguard and the means by which to obtain a copy of them or where they have been made available;

4.1.5. the period for which such personal data shall be stored or, if that is not possible, the criteria for determining such period;

4.1.6. the existence of the data subject's rights which are listed in paragraphs 6 below;

4.1.7. where processing is based on data subject consent, the right for the data subject to withdraw consent at any time;

4.1.8. the right to lodge a complaint with a supervisory authority;

4.1.9. whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; and

4.1.10. the existence of any automated decision-making, which produces legal effects concerning the data subject or similarly affects the data subject, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

4.2. If we receive personal data about a data subject from other sources, we shall provide the data subject with the information in paragraph 4.1 above, together with details of the categories of personal data concerned and the source of the personal data (and, if applicable, whether it came from a public source), as soon as possible thereafter.

4.3. We shall also inform data subjects whose personal data we process that we are the data controller with regard to that data and we shall provide contact details of the Data Protection Officer.

4.4. If we intend to further process the personal data for a purpose other than that for which the personal data was collected, we shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 4.1.

5 Consent

5.1. Where processing is based on consent, we will demonstrate that the data subject has consented to processing of his or her personal data.

5.2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, we shall present the request for consent in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

5.3. The data subject shall have the right to withdraw his or her consent at any time. Data users should consult with their line manager or the Data Protection Officer if they receive a notification that a data subject wishes to withdraw his or her consent.

5.4. When assessing whether consent is freely given by the data subject, utmost account shall be taken of whether, amongst other things, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

6 Data Subject rights

6.1. The right to be informed

6.1.1. The privacy notice supplied to individuals describing the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.

6.1.2. If services are offered directly to a child, we will ensure that the privacy notice is written in a clear, plain manner that the child will understand.

6.1.3. In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the information set out in paragraph 4.1 above will be supplied within the privacy notice:

6.1.4. Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement and the details of the categories of personal data, as well as any possible consequences of failing to provide the personal data, will be provided.

6.1.5. Where data is not obtained directly from the data subject, information regarding the source the personal data originates from and whether it came from publicly accessible sources, will be provided.

6.1.6. For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

6.1.7. In relation to data that is not obtained directly from the data subject, this information will be supplied:

6.1.7.1. Within one month of having obtained the data.

6.1.7.2. If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.

6.1.7.3. If the data are used to communicate with the individual, at the latest, when the first communication takes place.

6.2. The right of access

6.2.1. Individuals have the right to obtain confirmation that their data is being processed.

6.2.2. Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

6.2.3. We will verify the identity of the person making the request before any information is supplied.

6.2.4. A copy of the information will be supplied to the individual free of charge; however, we may impose a 'reasonable fee' to comply with requests for further copies of the same information.

6.2.5. Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

6.2.6. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged. All fees will be based on the administrative cost of providing the information.

6.2.7. All requests will be responded to without delay and at the latest, within one calendar month of receipt.

6.2.8. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

6.2.9. Where a request is manifestly unfounded or excessive, we have the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

6.2.10. In the event that a large quantity of information is being processed about an individual, we will ask the individual to specify the information the request is in relation to.

6.3. The right to rectification

6.3.1. Individuals are entitled to have any inaccurate or incomplete personal data rectified.

6.3.2. Where the personal data in question has been disclosed to third parties, we will inform them of the rectification where possible.

6.3.3. Where appropriate, we will inform the individual about the third parties that the data has been disclosed to.

6.3.4. Requests for rectification will be responded to within one calendar month; this will be extended by two months where the request for rectification is complex.

6.3.5. Where no action is being taken in response to a request for rectification, we will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

6.4. The right to erasure

6.4.1. Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

6.4.2. Individuals have the right to erasure in the following circumstances:

6.4.2.1. Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed;

6.4.2.2. When the individual withdraws their consent;

6.4.2.3. When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing;

6.4.2.4. The personal data was unlawfully processed;

6.4.2.5. The personal data is required to be erased in order to comply with a legal obligation;

6.4.2.6. The personal data is processed in relation to the offer of information society services to a child.

6.4.3. We have the right to refuse a request for erasure where the personal data is being processed for the following reasons:

6.4.3.1. To exercise the right of freedom of expression and information

6.4.3.2. To comply with a legal obligation for the performance of a public interest task or exercise of official authority

6.4.3.3. For public health purposes in the public interest

6.4.3.4. For archiving purposes in the public interest, scientific research, historical research or statistical purposes

6.4.3.5. The exercise or defence of legal claims

6.4.4. As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

6.4.5. Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

6.4.6. Where personal data has been made public within an online environment, we will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

6.5. The right to restrict processing

6.5.1. Individuals have the right to block or suppress our processing of personal data.

6.5.2. In the event that processing is restricted, we will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

6.5.3. We will restrict the processing of personal data in the following circumstances:

6.5.3.1. Where an individual contests the accuracy of the personal data, processing will be restricted until we have verified the accuracy of the data

6.5.3.2. Where an individual has objected to the processing and we are considering whether their legitimate grounds override those of the individual

6.5.3.3. Where processing is unlawful and the individual opposes erasure and requests restriction instead

6.5.3.4. Where we no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim

6.5.4. If the personal data in question has been disclosed to third parties, we will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

6.5.5. We will inform individuals when a restriction on processing has been lifted.

6.6. The right to data portability

6.6.1. Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

6.6.2. The right to data portability only applies in the following cases:

6.6.2.1. To personal data that an individual has provided to a controller;

6.6.2.2. Where the processing is based on the individual's consent or for the performance of a contract;

6.6.2.3. When processing is carried out by automated means.

6.6.3. Personal data will be provided in a structured, commonly used and machine-readable form. We will provide the information free of charge.

6.6.4. Where feasible, data will be transmitted directly to another organisation at the request of the individual.

6.6.5. We are not required to adopt or maintain processing systems which are technically compatible with other organisations.

6.6.6. In the event that the personal data concerns more than one individual, we will consider whether providing the information would prejudice the rights of any other individual.

6.6.7. We will respond to any requests for portability within one calendar month.

6.6.8. Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

6.6.9. Where no action is being taken in response to a request, we will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

6.7. The right to object

6.7.1. Individuals have the right to object to the following:

6.7.1.1. Processing based on legitimate interests or the performance of a task in the public interest;

6.7.1.2. Direct marketing;

6.7.1.3. Processing for purposes of scientific or historical research and statistics.

6.7.2. Where personal data is processed for the performance of a legal task or legitimate interests:

6.7.2.1. An individual's grounds for objecting must relate to his or her particular situation.

6.7.3. We will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

6.7.4. Where personal data is processed for direct marketing purposes:

6.7.4.1. We will stop processing personal data for direct marketing purposes as soon as an objection is received.

6.7.4.2. We cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

6.7.5. Where personal data is processed for research purposes:

6.7.5.1. The individual must have grounds relating to their particular situation in order to exercise their right to object.

6.7.6. Where the processing of personal data is necessary for the performance of a public interest task, we are not required to comply with an objection to the processing of the data.

6.7.7. Where the processing activity is outlined above, but is carried out online, we will offer a method for individuals to object online.

7 Data Security[2]

7.1. We shall put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data shall only be transferred to data processors if they agree to comply with those procedures and policies, or if they put in place adequate measures themselves.

7.2. We shall maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

7.2.1. Confidentiality means that only people who are authorised to use the data can access it.

7.2.2. Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.

7.2.3. Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual PCs.

7.3. Security procedures include:

7.3.1. Entry controls: Any unfamiliar person seen in entry-controlled areas should be reported.

[2] Please see our IT Security Policy

7.3.2. Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind (personal information is always considered confidential).

7.3.3. Methods of disposal: Paper documents should be shredded. Digital storage devices should be physically destroyed or wiped when they are no longer required.

7.3.4. Equipment: Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

8 Data Processors

8.1. We shall only use processors who provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the law and ensure the protection of the rights of the data subject.

8.2. Our contracts with data processors shall set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.

8.3. Our contracts with data processors shall stipulate that the processor:

8.3.1. processes the personal data only on our documented instructions;

8.3.2. ensures that persons authorised to process the personal data are subject to appropriate confidentiality obligations;

8.3.3. takes all measures required to ensure the security of the personal data [including complying with our Information and Security Management Policy;

8.3.4. shall not engage another processor without our prior written consent, and where another processor is engaged, it must be subject to obligations equal to obligations imposed on the original processor, and the original processor must remain fully liable to us for performance of its data protection obligations;

8.3.5. assists us by using appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of our obligation to respond to requests for exercising the data subject's rights;

8.3.6. assists us to comply with our obligations under the Data Protection Legislation;

8.3.7. shall, at our discretion, delete or return personal data at the end of the service provision (unless required by law to store the personal data);

8.3.8. makes available to us all information necessary to demonstrate its compliance with its data protection obligations in its contract with us; and

8.3.9. shall keep a written record (which may be in electronic form) of all processing activities, which it shall make available to a supervisory authority on request, containing the following information:

8.3.9.1. the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the Data Protection Officer;

8.3.9.2. the categories of processing carried out;

8.3.9.3. where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, if applicable, the documentation of appropriate safeguards; and

8.3.9.4. where possible, a general description of the technical and organisational security measures which are in place to protect personal data.

9 Transferring Personal Data to a Country Outside the EEA

9.1. We may transfer any personal data we hold to a country outside the European Economic Area ("EEA"), provided that one of the following conditions applies:

9.1.1. the country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms;

9.1.2. the data subject has given his/her consent;

9.1.3. the transfer is necessary for one of the reasons set out in the Data Protection Legislation, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject;

9.1.4. the transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims; or

9.1.5. the transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

9.2. Subject to the requirements in paragraph 9.1 above, personal data we hold may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. That staff maybe engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

10 Disclosure and Sharing of Personal Information

10.1. We may share personal data we hold with any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries, as defined in section 1159 of the UK Companies Act 2006.

10.2. We may disclose personal data we hold to third parties:

10.2.1. In the event that we, our business, or substantially all of its assets are acquired by a third party (in which case personal information about customers will be one of the transferred assets); or

10.2.2. if we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

10.3. We may share personal data with data processors in accordance with the terms of this policy.

10.4. We may share personal data we hold with selected third parties upon obtaining appropriate consent of the data subject.

PART 2: DATA RETENTION

11 Principles

11.1. Personal data should only be retained for as long as necessary. The retention periods can differ based on the type of data processed, the purpose of processing or other factors. Issues to consider include:

11.1.1. Whether any legal requirements apply for the retention of any particular data. For example:

11.1.1.1. Tax law;

11.1.1.2. Employment law;

11.1.1.3. Litigation law;

11.1.1.4. Regulations and guidance from regulators.

11.2. In the absence of any legal requirements, personal data may only be retained as long as necessary for the purpose of processing. This means data is to be deleted e.g. when:

11.2.1. the data subject has withdrawn consent to processing;

11.2.2. a contract has been performed or cannot be performed anymore; or

11.2.3. the data is no longer up to date.

11.3. Other issues to consider:

11.3.1. Has the data subject requested the erasure of data or the restriction of processing?

11.3.2. Is the retention still necessary for the original purpose of processing?

11.3.3. How recently was consent given?

11.3.4. Does the legitimate interest (where relevant) still override the rights of the data subject?

11.3.5. Exceptions may apply to the processing for historical, statistical or scientific purposes.

11.4. During the retention period

11.4.1. We will establish periodical reviews of data retained.

11.4.2. In establishing and verifying retention periods for data we will consider the following categories:

11.4.2.1. the requirements of our business;

11.4.2.2. type of personal data;

11.4.2.3. purpose of processing;

11.4.2.4. lawful grounds for processing;

11.4.2.5. categories of data subjects; and

11.4.2.6. any legal or regulatory requirements.

11.4.3. If precise retention periods cannot be established, we will identify criteria by which the period can be determined.

11.5. Expiration of the retention period

11.5.1. After the expiration of the applicable retention period we will either:

11.5.1.1. erase the relevant personal data; or

11.5.1.2. anonymise the data.

11.5.2. In erasing data, we will ensure that relevant archived, backup and deleted personal data are also erased, including any archived data held outside the company. In the event that this is not possible, we will ensure that:

11.5.2.1. the personal data is beyond use;

11.5.2.2. we will not use or attempt to be use the personal data to inform any decision in respect of any natural person;

11.5.2.3. No other organisation is given access to the personal data;

11.5.2.4. appropriate technical and organisational measures for security are in place; and

11.5.2.5. we will permanently erase the personal data if or when this becomes possible.

11.5.3. In anonymising data we will use the following techniques:

11.5.3.1. erasure of the unique identifiers which allow the allocation of a data set to a unique person;

11.5.3.2. erasure of single pieces of information that identify the data subject (whether alone or in combination with other pieces of information);

11.5.3.3. separation of personal data from non-identifying information (e.g. an order number from the customer's name and address); or

11.5.3.4. aggregation of personal data in a way that no allocation to any individual is possible.

11.6. Information obligations

11.6.1. In addition to other information obligations, in the context of data retention we will inform data subjects of:

11.6.1.1. the retention period;

11.6.1.2. if no fixed retention period can be provided – the criteria used to determine that period; and

11.6.1.3. the new retention period if the purpose of processing has changed after personal data has been obtained.

12 Data storage & retention

12.1. All personal data will be stored securely in order to avoid potential misuse or loss.

12.2. Personal data will be stored in the most convenient and appropriate location having regard to the period of retention required and the frequency with which access will be made to the record and limited to the individuals that require access.

12.3. The degree of security required for file storage will reflect the sensitivity and confidential nature of any material recorded. However all personal data and records should be readily accessible and retrievable in an acceptable format to allow authorised requests for information to be fulfilled in a timely manner.

12.4. Personal data will not be kept longer than is necessary for its purpose except where retention is required by statute. This means that we will destroy, erase or de-personalise data when it is no longer required for statutory purposes or to fulfil the legal purpose(s) for which it was obtained or required for business continuity purposes.

12.5. Any requests submitted by customers or employees to erase personal data will be reviewed by the DPO against the statutory requirements and our legitimate business interests.

12.6. We will adhere to **Appendix 1**, which shows how long certain categories of data, including personal data, will be kept.

12.7. At the end of the prescribed retention period, we may de-personalise and archive electronic data for the purposes of statistical analysis. All personal data that could identify an individual will be removed. Any records held on hard media, CD, DVD, paper or any scanned documents that cannot be de-personalised will be destroyed.

12.8. We may limit the de-personalisation of data where customers have provided their consent for us to retain their personal data beyond the prescribed retention period.

13 Application of the retention rules

13.1. The retention rules shown in Appendix 1 apply to both hard and soft formats that are used to store personal records for customers and employees. We will keep the data for as long as the customer or employee has a relationship with us and the retention period shown in the schedule will begin when that relationship ends.

13.2. For the purposes of retention, the relationship with the customer ends when we have completed the work for which we contracted with the customer.

13.3. For the purposes of retention, the relationship with the employee ends on their last contracted date of employment and the relationship with an unsuccessful job applicant ends when the recruitment process ends for the role they applied for.

13.4. Each department must carry out regular reviews of the data they store and consider confidentially destroying data that is not required.

14 How to make a complaint

14.1. If you are unhappy with the way in which your personal data has been processed you may in the first instance contact the Data Protection Officer using the contact details Data Protection Officer, Level 30, One Canada Square, Canary Wharf, London E14 5AB.

14.2. If you remain dissatisfied then you have the right to apply directly to the Information Commissioner for a decision. The Information Commissioner can be contacted at:

The Information Commissioner, Wycliffe House, Water Lane, Wilmslow Cheshire SK9 5AF
Telephone: Switchboard: 01625 545 700
Data Protection Help Line: 01625 545 745
Notification Line: 01625 545 740
Email: mail@ico.gsi.gov.uk

15 About this Policy

15.1. The types of personal data that we may be required to handle include information about current, past and prospective suppliers, clients, customers, employees, and others that we communicate with. The personal data is subject to certain legal safeguards which are specified in the Data Protection Act 2018 and other regulations, including the General Data Protection Regulation.

15.2. This policy, together with any other documents referred to herein, sets out the basis on which we will process personal data, and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

15.3. This policy does not form part of any employee's contract of employment and may be amended by us at any time.

15.4. The Data Protection Officer (contactable via DataProtection@canarywharf.com) is responsible for ensuring compliance with the data protection laws and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Officer.

15.5. We reserve the right to change this policy at any time. Where appropriate, we shall notify subjects of this policy of those changes by e-mail or update on our intranet.

15.6. This policy was last updated in May 2018.

APPENDIX 1: Retention of records

1. Human Resources and Payroll Records

1.1 We have regard to recommended retention periods for particular employment records as set out in legislation, referred to in the table below. However, it also has regard to legal risk and may keep records for up to seven years (and in some instances longer) after the relationship with the employee or job applicant ends.

Record	Retention period
Accounting records	**3 years** for private companies, **7 years** for public limited companies
Actuarial valuation reports	Permanently
Application forms, CVs and interview notes, assessment exercises or tests, pre-employment verification details, criminal records checks (for unsuccessful candidates)	**6 months**
Children related records	**7 years** from date of termination of parent (employee's) employment
Deferred pensioners' records	Until benefit ceases
Immigration checks	Indefinitely after termination of employment
Inland Revenue approvals	Permanently
Maternity Pay records, calculations, certificates (Mat B1s) or other medical evidence, dates of maternity leave, period without maternity payment	**7 years** after the end of the tax year in which the maternity period ends
Parental leave	**7 years** from birth/adoption of the child or **18 years** if the child receives a disability allowance
PAYE/Income tax and NI returns, income tax records and correspondence with the Inland Revenue, hours worked and payments or loans made	7 **years** after the end of employment
Payroll/wage records (also overtime, bonuses, expenses, benefits in kind)	**7 years**
Pension records relating to events notifiable under the Retirement Benefits Schemes (Information Powers) Regulations 1995, records concerning decisions to allow retirement due to incapacity, pension accounts and associated documents or money purchase records	**7 years** from the end of the scheme year in which the event took place, or the date upon which the accounts/reports were signed/completed
Pension scheme investment policies	**12 years** from the ending of any benefit payable under the scheme
Personnel files and training records (including disciplinary and grievance records, working time records, training, leave records, qualifications, references, resignation, termination, retirement contracts, written particulars of employment and changes to	**7 years** after employment ceases

terms and conditions)	
Redundancy details, calculations of payments, refunds, notification to the Secretary of State	**7 years** from the date of redundancy
Staff consultative committee	**7 years**
Statutory Sick Pay records, calculations, certificates, self-certificates	**7 years** after the end of the tax year to which they relate
Time cards/sheets	**3 years** after audit
Trust deeds and rules and trustees minute books	Permanently

2. Health and Safety Records

Record	**Retention period**
Accident/Incident Investigations	**3 years** or **40 years** for incidents involving hazardous substances e.g. asbestos exposure, exposure above the Workplace Exposure Limit (WEL)
Accident/Incident reports	**3 years** from date of incident For incidents involving minors – up to 22 years (applying the entitlement of a child to bring a claim up to **3 years** after their 18th birthday)
Audit Records	**6 years**
Business Continuity plans	**5 years**
CDM Documentation	**5 years**
Certification/Accreditation	**5 years**
Confined Spaces register	**5 years**
Contractor documentation (including Safecontractor)	**5 years**
Control of Substances Hazardous to Health / Hazardous Substances Assessments	Until revised
Display Screen Equipment Assessments	**5 years**
Enforcement notices / communication with enforcing body	**5 years**
Environmental records	**5 years**
Equipment testing records (including calibration, PAT etc.)	**5 years**
Fire Equipment Records	**5 years**
Fire Evacuation Records	**3 years**

Fire Risk Assessments	**3 years**
First Aid & defibrillator equipment records	**3 years**
First Aid Assessment	**3 years**
First Aider lists	**3 years**
H&S File	Lifespan of the building
Health & Safety Policy	Until superseded
Health & Safety Procedures	Until superseded
Health & Safety Strategy	**3 years**
Health & Safety training	**10 years**
Health surveillance and medical records plus air monitoring and/or biological monitoring etc, kept by reason of the Control of Substances Hazardous to Health Regulations 2002	**40 years**
Inspection Records	**6 years**
Legionella Policy	Until superseded
Meeting minutes (I.e. HoD, Engineers meeting)	**3 years**
New & Expectant Mothers Risk Assessment	Date of notification of pregnancy **+ 22 years** (unless exposure to hazardous substances and physical agents in which case + 40/50)
Objectives	**3 years**
Occupational Health Records - health surveillance and medical records relating to risk assessments or incidents occurring at work	**40 years**
Occupational Health Records where reason for termination of employment is connected with health, including stress related illness	During employment plus **3 years**
Permit to Work records	**7 years** after cancellation
Personal Emergency Evacuation Plans	Until superseded
Personal Protective Equipment – safety clothing and hardware	Retain for duration of work on site
Personal Protective Equipment records	**5 years**
Personal Risk Assessments	**10 years**
Physical agents – including Whole Body and Hand Arm vibration	**40 years**
Physical agents – Ionising radiation	**50 years** after last entry

Records relating to asbestos, medical records, training records, suspect incidents of potential exposure	**40 years**
Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR) reports	**3 years** from date of notification
Return To Work Assessments	**10 years**
Risk Assessments – task and activity based	**5 years** or as long as the task/activity is performed/until superseded
Safety Representatives	**3 years**
Statutory testing records (LOLER, PUWER etc.)	As long as equipment is being operated + 2 years
Water management records (including testing)	**5 years**
Young Persons Assessments	Date joined + **5 years**

3. Security Records

Record	**Retention period**
Access Control System (CCure)	**3 years** and 3 months
Audio Recordings (Including Redbox, Stentofon, TUBONet)	**28 Days** - (unless authorised for a justified retention period by the Data Controller)
Banning Notice Database	Length of Ban
CCTV Cameras (including Body Worn Video and)	**28 Days** - (unless authorised for a justified retention period by the Data Controller)
Contact Lists (Including Tenants and Staff)	Bi-annually and in accordance with policy
Contract Staffing (VSG, Magenta, ICTS)	**7 years** after termination of individual or corporate contract
Incident Management System ((IMS) ISARR)	**5 Years** - To be reviewed on retention
Intelligence (including Search Databases, Open Source Research, Reports)	**3 years**
Mass Messaging (Estate Alert / Public Address Systems)	As soon as no longer required
Operational Documentation (including Notebooks, Accident Reports, Insurance Forms, Banning Notices, Rosters, Break Logs, Lost and Found Property)	All except Rosters, Break Logs and Lost and Found to be entered on to the IMS and destroyed. These exceptions are only to be retained as long as necessary
Payroll and Canary Wharf Staffing (Crown)	**7 years** – after termination of individual or corporate contract
Recruitment (including CV's, applications and interview notes)	**6 months**
Security Briefing System	As soon as no longer required

Staff Personal Files (including Appraisals, Probation Reports, Return to Work, Absence Records, Discipline Records, File Notes, Investigations, Risk Assessments, Acting Promotion Data, Leave Requests, Personal Risk Assessments, Equipment Issue, Physical Employment Standards (PES))	**7 years** - after employment ends. Any paper document is to be scanned and stored in an identifiable folder, and / or uploaded on to the IMS where applicable and forwarded to HR for storing on the individuals personnel file
Training (including records and reports)	**7 years**

4. Client/Supplier Records

Record	**Retention period**
Accounting records These include: Payment details Transaction details File copies of bills and costs delivered, including fees and disbursements shown separately Bank statements	**7 years** after the relevant date
Returned cheques Copies of payment instructions (confirmed in writing)	**2 years** from the relevant date of the transaction
Warranties, indemnities and guarantees	At least **7 years** from the date of completion of the construction
Records relating to the tender process These may include: Pre-qualification details Successful tender applications Unsuccessful tender applications Tender reports, recommendations etc Tender documentation Design consultant proposals (successful or otherwise)	**7 years** from date of completion of the construction