Data Protection Policy

Responsible Officer	Russell Hall, Director of Governance
This policy is applicable to	Group
Approved by	Karbon Management Team
Date approved	28th August 2025
Frequency of review	Every 3 years or if there is a significant change in legislation, regulation or guidance.
Date of next review	28th August 2028
Implementation date	29th August 2025
Key related documents	Data protection procedures Disciplinary policy Disposal log Document Retention and Disposal Schedule Register of Processing Activities
Sources of best practice or guidance used in developing this policy	Information Commissioners Office IT Governance Muckle LLP

Version control			
Version number	1.7	Author of Policy	Jill Johnson, Senior Data Protection Business Partner
Equality Impact Analysis	Initial	Equality Analysis Date	31st March 2019

Document change history		
Version	Date	Changed sections
1.0	13/04/2018	New Karbon Policy incorporating GDPR
1.1	03/07/2018	Sections 3.7 and 3.13 amended after guidance from Muckle LLP and the enactment of the Data Protection Bill 2018.
1.2	23/10/2018	Section 3.2, Breaches amended to indicate that colleagues should report breaches as soon as they are aware of them and without delay.
1.3	31/03/2019	Annual policy refresh
1.4	04/02/2020	Policy refresh to include Company Confidential/Sensitive Data
1.5	14/07/2021	Amended GDPR to UK GDPR, 3.10 expanded
1.6	29/05/2022	3.10 and 3.25 amended to reflect audit actions
1.7	31/07/2025	New sections added on: Accuracy, Artificial Intelligence/Large Language Models, Complaints, DPIA, Imagery and associated sound recordings, Information

		classification, Record Keeping, Responsibilities, ROPA, Supervisory Body, Surveys, Third Party requests (replacing disclosure and sharing), Further Information. Amended separate mentions of UK GDPR and DPA to Data Protection Legislation to also incorporate PECR and DUAA.

Consultation	
Consultation Group	Date of Consultation
Colleague forum	04/06/2025
Comms and Marketing	26/06/2025
Housing	16/06/2025
POD	04/06/2025
Health and Safety	04/06/2025
Information Governance	05/06/2025
Procurement	04/06/2025
Governance	04/07/2025
EDI	06/06/2025
ICT	05/06/2025
Customer Services	04/06/2025
Customer Experience	04/06/2025
Other stakeholder (please state)	Muckle LLP: 23/08/18; 06/06/2018

Policy statement

During your employment, you may process Personal or Company Confidential/Sensitive Data on behalf of The Group and The Group will process Personal Data about you. You are obliged to comply with this policy when Processing Personal or Company Confidential/Sensitive Data on behalf of The Group and any breach of this policy may result in disciplinary action.

In order to operate and carry out its functions, The Group needs to process information and keep records, this information may be classed as Company Confidential/Sensitive Data, or it could relate to the people with whom it interacts. This may include members of the public, current past and prospective employees, customers and suppliers for legal, personnel, administrative and management purposes and to enable us to meet our legal obligations as an employer, for example, to pay you and to confer benefits in connection with your employment.

The Group is fully committed to full compliance with the requirements of Data Protection legislation.

The Group will follow procedures which aim to ensure that all Data Users who have access to any Personal Data or records held by, or on behalf of, The Group are fully aware of and abide by their duties under Data Protection legislation. This will be done irrespective of the way in which the personal information is collected, recorded or used and whether it is on paper, in computer records or recorded by other means.

Everyone has rights regarding the way in which their Personal Data is processed and we recognise that the correct and lawful treatment of this Data will maintain confidence in The Group and will provide for successful business operations.

The Group will assist Data Subjects in exercising their rights under Data Protection legislation, ensuring that Personal Data is lawfully processed in accordance with the six 'Data Protection Principles' as well as being accountable as per a seventh principle, with information only being held for the time required to complete its specified purpose and its associated retention period.

The Senior DPBP is responsible for ensuring compliance with Data Protection legislation and with this Policy. That post is held by Jill Johnson and 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 Senior DPBP.

This policy does not form part of any employee's contract of employment, and we may amend it at any time.

Risk policy is designed to control

9.2b: Cyber Resilience and Data Protection

This policy seeks to clarify the rules around data protection for Personal Data and highlights The Group and its employees' obligations regarding Personal or Company Confidential/Sensitive Data.

This will help to reduce the reputational and financial risks faced by The Group due to the lack of protection of Personal or Company Confidential/Sensitive Data processed in the course of its business.

This constitutes a significant financial and reputational risk.

Key performance measures

- 100% of subject access requests completed within a calendar month.
- Number of reported breaches.
- Number of near misses.

Abbreviations

- DPBP: Data Protection Business Partner
- DPIMC: Data Protection & Information Management Coordinator
- IC: Information Commission
- The Group: Karbon Homes and all subsidiaries

Definitions

- **Artificial Intelligence (AI):** a computer system designed to perform tasks that typically need human intelligence, such as speech recognition, decision making, and pattern identification.
- **Company Confidential/Sensitive Data** – this is data (which may also contain Personal Data) which could have a negative impact on The Group or its reputation if it were made available to the public or third parties.
- **Consent (of the Data Subject)** - any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her.

- **Customer** - any individual who has or requests a service from The Group.
- **Data** - information which is stored electronically, on a computer, or in certain paper-based filing systems.
- **Data Controller** - the people who or organisations which alone or jointly with others determine the purposes, conditions and means of the Processing of Personal Data. They are responsible for establishing practices and policies. We are the Data Controller of all Personal Data used in our business for our own commercial purposes.
- **Data Processor** - any person or organisation that is not a Data User that processes Personal Data on behalf of the Data Controller.
- **Data Protection legislation:** includes but is not limited to: UK GDPR, DPA 2018, PECR 2003 and the DUAA 2025.
- **Data Subject** - a living person whose Personal Data is processed by a controller or processor. A Data Subject need not be a UK national or resident. All Data Subjects have legal rights in relation to their personal information.
- **Data User** - any colleague, contractor, consultant or person who has access to any Personal Data held by or on behalf of The Group. Data Users must protect the Personal Data they handle in accordance with this policy and any applicable Data security procedures at all times.
- **Imagery and associated sound/voice recording**s: any photographic images, video footage, audio, or video stills.
- **Information** – a collection of data organised or processed to give context. This could be in the form of documents, records, or other content.
- **Large Language Models (LLM):** A Large Language Model (LLM) is a type of artificial intelligence algorithm that applies neural network techniques with extensive parameters to process and understand human languages or text using self-supervised learning techniques
- **Personal Data** - any information relating to an identified individual (i.e. which makes such information personal to that individual), or any information relating to someone who could be identified based on a variety of identifiers such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, biometric, mental, economic, cultural or social identity of that natural person. Personal Data can be factual or an opinion about that person, their actions and behaviour.
- **Processing/Processing Activity** - 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.
- **Special Category Data** - Processing of Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the Processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, Data concerning health or Data concerning a natural person's sex life or sexual orientation shall be prohibited. Special Category Data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

- **Stakeholder** – a person, group or organisation that has interest or concern in The Group or its activities. Stakeholders can affect or be affected by The Groups actions, objectives and policies.

1.0 Purpose of the policy

1.1 As the general Data Protection policy of The Group this document outlines how data protection will be incorporated into its management structure and the responsibilities that it involves for colleagues at all levels of the organisation.

1.2 The Group needs to collect and use information that could be considered Company Confidential or Sensitive Data as well Personal and Special Category Data in order to operate. This procedure has been written to ensure that The Group has safeguards in place to protect all types of Data and its acceptable use.

1.3 In terms of what information is in scope for this Group policy, it could be any information relating to its current, past or prospective; employees, suppliers, tenants, leaseholders, clients, customers, third party organisations, Stakeholders or anyone else The Group communicates with or processes information to or on behalf of. Data Protection legislation requires that this personal information must be dealt with properly when it is processed - whether on paper, in a computer or recorded on other material.

1.4 This policy sets out how The Group will protect information ensuring that colleagues understand the rules governing the information which they have access to in the course of their work.

1.5 In particular, this policy requires colleagues to ensure that the Senior DPBP or Senior DPIMC is consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

2.0 Objectives

2.1 The objectives of the Policy are to ensure that all colleagues:

- are aware of their own individual as well as Group wide responsibilities when it comes to the processing of Personal, Special Category and Company Confidential/Sensitive Data; and
- know where to locate and who to contact to discuss any data protection related items or to get support or guidance for the activities they are performing that involve Data.

3.0 Policy detail

3.1 **Accuracy**

Colleagues will ensure that any Personal Data processed by The Group is accurate and, in accordance with the Data Subject's Right to Rectification, take reasonable steps to destroy, delete or amend inaccurate or out of date Personal Data without undue delay.

On becoming aware of an inaccuracy in Personal or Special Category Data, colleagues should take steps to ensure that it is corrected as soon as possible - taking into consideration any external requirements such as proof of name change.

As a colleague of The Group, if your personal details change or if you become aware of any inaccuracies in the Personal Data processed by The Group relating to you or a family member, then it is your responsibility to ensure that it is corrected.

Whilst some details can be amended through the 'self-serve' functionality of our iTrent system, there may be some that must be completed via your manager and/or POD and may require further information to action.

3.2 **Artificial Intelligence / Large Language Models:**

The Group will ensure that any Artificial Intelligence or Large Language Model system it uses is designed and implemented in a manner that respects privacy whilst also adhering to the principles of data protection.

Colleagues will ensure that they do not use, for work purposes, any Artificial Intelligence or Large Language Model system unless permitted for use by The Group.

Colleagues must consult with the Senior DPBP/DPIMC and ICT before deploying any Artificial Intelligence or Large Language Model solution, to ensure compliance with Data Protection and ICT regulations and requirements as well as safeguarding sensitive information.

Further information can be found in the ICT Acceptable Use Policy.

3.3 **Breaches**

It is the responsibility of each colleague to report actual or potential data protection compliance failures as soon as they are aware of them and without delay to the data protection email mailbox. This allows us to:

- investigate the failure and take remedial steps if necessary;
- maintain a register of compliance failures;
- identify trends in breaches;
- learn from our mistakes and improve service delivery;
- notify the IC of any compliance failures that are material either in their own right or as part of a pattern of failures; and
- ensure that we report any breaches without undue delay.

Further guidance on breaches can be found in the Data Breach Incident procedure.

3.4 **Children**

Colleagues will need to ensure that when they are Processing Personal Data regarding children that they have an appropriate lawful basis for doing so.

If the lawful basis is Consent, it must be assured that if the child is aged 13 or over that the Consent is from the child themselves and that special measures may need to be taken to ensure that the child is fully aware of what they are consenting to. For children aged under 13, the Consent should be from whomever has parental responsibility.

3.5 **Complaints**

Any concerns about Data Protection should be raised initially with a member of the Data Protection team at data.protection@karbonhomes.co.uk who can give advice and manage the actions that should be taken.

Everyone has the Right to Complain to our Supervisory body, the IC if they feel that we have not dealt with their request for information properly or are concerned about the way we are Processing their Personal Data.

This Right does not apply to the service they receive from the Data Protection team as these types of complaints would be managed in accordance with The Group Complaints Policy.

3.6 **Consent**

Some of the Personal Data that we collect is subject to active Consent by the Data Subject and this consent can be revoked at any time. We will record for what purpose Consent is given along with the method used to give Consent and when it was given, we will also record this information when consent is withdrawn.

Further guidance on Consent can be found in the Consent procedure.

3.7 **Criminal convictions and offences**

Colleagues will act in accordance with Data Protection legislation when processing information relating to a Data Subjects criminal offences and behaviours.

Only information relating to unspent offences and behaviours will be processed.

Colleagues are only able to ask a Data Subject about their criminal offences or behaviours if it is required to enter into or remain in a contract with The Group. Requesting this information for any other purpose should be confirmed with the Senior DPBP/DPIMC before the request or processing takes place as alternative purposes may not have a lawful basis for processing.

Colleagues should not share information relating to criminal offences and behaviours with third parties unless it relates to the Data Subject entering into or remaining in a contract with The Group. If in doubt, clarification must be sought from the Senior DPBP/DPIMC before information is shared.

3.8 **Data portability**

Upon request, a Data Subject has the right to receive a copy of their data in a structured format. These requests should be processed within one calendar month, provided there is no undue burden, and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done for free.

3.9 **Data Protection Impact Assessment (DPIA)**

Before we carry out any processing, we must consider data protection through a series of mandatory screening questions known as a Data Protection Impact Assessment (DPIA) this is an integral part of the 'Privacy by Design' approach, required under Data Protection legislation

By conducting a DPIA The Group can identify potential data protection issues at an early stage, enabling solutions to be put in place to reduce, mitigate or remove the reputational and financial risks of the processing.

Further information can be found in the DPIA procedure.

3.10 **Data Protection principles**

We will process Personal Data in compliance with all six Data Protection principles which are that Personal Data must be:

a) processed lawfully, fairly and in a transparent manner in relation to the Data subject ('lawfulness, fairness and transparency');

b) 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, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

d) 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 ('accuracy');

e) 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 in accordance with Article 89 (1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the Data Subject ('storage limitation'); and

f) 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 ('integrity and confidentiality').

There is a further seventh principle which is that: 'the controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (accountability)' this means that The Group must be able to demonstrate compliance with the first 6 principles.

3.11 **Data retention and disposal**

Colleagues must not retain Personal Data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the Personal Data was obtained, but should be determined in a manner consistent with our Document Retention and Disposal Schedule.

When disposing of printed, photocopied or handwritten documents/notes that may contain Company Confidential/Sensitive Data or Personal Data, colleagues will ensure that they use one of the locked shredding boxes or shredding bags found in the offices and not a normal or recycling waste bin. This will help ensure that no unauthorised party would be able to access, view or further process the data and reduce instance of data breaches.

Colleagues will ensure that when disposing of Data, they record it in the Disposal Log and, if a third party is used for disposing of the Data, obtain a Certificate of Disposal if necessary. Colleagues will take all reasonable steps to destroy, or erase from our systems, all Data which is no longer required.

Further guidance on data retention and disposal can be found in the Retention and Disposal procedure.

3.12 **Data security**

Colleagues will take appropriate security measures against unlawful or unauthorised Processing of Company Confidential/Sensitive Data or Personal Data, and against the accidental loss of, or damage to, Company Confidential/Sensitive Data or Personal Data.

The Group will put in place procedures and technologies to maintain the security of all Company Confidential/Sensitive Data or Personal Data from the point of collection to the point of destruction. Personal Data will only be transferred to a Data Processor if they agree to comply with those procedures and policies, or they put in place adequate measures themselves.

Colleagues must keep Company Confidential/Sensitive Data or Personal Data secure against loss or misuse. Where other organisations process Personal Data as a service on our behalf, the Contract Manager with input from the Senior DPBP/DPIMC will establish what, if any, additional specific Data security arrangements need to be implemented in contracts with those third-party organisations through a Data Processing/Sharing Agreement.

3.13 **Direct marketing**

Colleagues must abide by any request from an individual not to use their Personal Data for direct marketing purposes and this should be recorded. Consent that is received for a purpose other than marketing cannot be used as consent to send marketing materials.

Do not send direct marketing material to someone electronically (e.g. via email) unless you have an existing business relationship with them in relation to the services being marketed.

Further guidance on Direct Marketing can be found in the External Communications and Marketing (Customer and Stakeholder) Policy.

3.14 **File transfer**

We will use appropriate technologies and software to ensure that when transferring Company Confidential/Sensitive Data or Personal Data that the methods used:

- secure the transmission of the Data through encryption;
- are password protected;
- provide a full audit trail; and
- scan transfers for malware.

3.15 **Indexing**

Personal information and records will be indexed in a logical manner which ensures ease of retrieval.

3.16 **Imagery and associated sound/voice recordings**

The processing of imagery relating to properties e.g. imagery showing an external view, a repair or the condition of property, does not require a lawful basis to allow its processing if it is ensured that no Personal Data - such as vehicle registration number, family photographs or a customer is recorded within the imagery.

On creation and during its ongoing storage, a valid lawful basis (for instance Consent) must be in place for any Imagery that captures a Data Subject and/or their associated sound/voice recordings – the exception to this is if the imagery is of historical importance.

We can retain the Imagery of Data Subjects and/or their associated sound/voice recordings whilst we have a lawful basis in line with our Data Retention and Disposal Schedule.

Once no lawful basis exists it must be deleted/destroyed. This means that if Consent was the lawful basis used and it was withdrawn, the imagery would need to be deleted/destroyed unless another valid lawful basis could be found to allow its continued processing.

Having a lawful basis for the use of a Data Subjects Imagery and/or their associated sound/voice recordings for one purpose, does not automatically mean that it can be used for an alternate purpose.

If no lawful basis exists specifically for the purpose you want to use the Data Subject imagery and its associated sound/voice recordings for, the imagery cannot be used.

Further information can be found in the Imagery procedure and Surveillance Camera Systems Personal Data procedure.

3.17 **Information Classification**
All information should be classified, valued and risk assessed in accordance with its confidentiality, integrity, and availability; regardless of the media on which it is stored, the manual or automated systems that process it, or the methods by which it is distributed.

Further information can be found in the Information Classification procedure.

3.18 **Justification for Personal Data**
We will document the justification for Processing Personal Data and will record the additional justification for the Processing of Special Category Data ensuring that any biometric and genetic data is considered special category within the Register of Processing Activities.

3.19 **Lawful Basis of Processing / Conditions for Processing**
We will ensure any use of Personal Data is justified using at least one of the Conditions for Processing and this will be specifically documented in the Register of Processing Activities.

All colleagues who are responsible for Processing Personal Data will be aware of the conditions for Processing. The conditions for Processing will be available to Data Subjects in the form of a privacy statement found on our website which is available electronically or in paper format on request.

The conditions for Processing are only deemed lawful if, and only to the extent that, at least one of the following applies:

a) "The Data Subject has given consent to the Processing of his or her Personal Data for one or more specific purposes" *(consent for a specific purpose has been given)*;

b) "Processing is necessary for the performance of a contract which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract" *(it is necessary for a contract the Data Subject is in or is asking to enter)*;

c) "Processing is necessary for compliance with a legal obligation to which the controller is subject" *(it is required for Karbon Homes compliance with a legal obligation)*;

d) "Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person" *(the vital interests of the Data Subject or another person are at risk)*;

e) “Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller” *(the Processing is in the public interest or a requirement of the controller’s official authority)*; and

f) “Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subjects which require protection of Personal Data, in particular where the Data Subject is a child” *(if The Group has a legitimate reason for Processing it we can unless it risks the Data Subject’s fundamental rights or freedoms)*.

Colleagues will not process Personal Data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

When Special Category Data is being processed, additional conditions must be met and, when Processing Special Category Data as a Data Controller, colleagues will ensure that those requirements are met.

Further guidance on Lawful Basis of Processing / Conditions of Processing can be found in the Lawful Basis procedure.

3.20 **Privacy statement**

Being transparent and providing accessible information to Data Subjects about how their Personal Data is being used is important for our organisation.

As well as being available in writing or electronically, our Privacy Statement is found on our website, and it contains information on:

- The name and contact details of the organisation as well as the person responsible for data protection;
- the purpose or purposes for which we intend to process Personal Data;
- the types of third parties or recipients, if any, with which we will share or to which we will disclose Personal Data;
- the lawful basis for the processing, sharing and/or disclosure of Personal Data;
- the retention periods for the Data;
- Data Subjects Rights including the Right to lodge a complaint with the IC; and
- the means, if any, with which Data Subjects can limit our use and disclosure of their Personal Data.

3.21 **Processing for Limited Purposes**

We will only process Personal Data for the purposes as agreed between the respective parties or specifically permitted by Data Protection legislation. We will notify those purposes to the Data Subject when we first collect the Data or as soon as possible thereafter.

We will only process your Personal Data as our employees for the specific purpose or purposes notified to you or for any other purposes specifically permitted by Data Protection legislation.

We will only collect Personal Data to the extent that it is required for the specific purpose notified to you as our employee or the Data Subject.

3.22 **Record Keeping**

When appropriate, colleagues should record interactions with Data Subjects in a timely manner and on the appropriate system e.g. Capita CRM for tenants.

When recording interactions, it is important that colleagues ensure that the note clearly indicates the date/time of the interaction (considering that this note may not be added straight after the interaction but a short time after); who was present, what was discussed, the actions that were agreed (or not), items they may have seen or heard that were of concern (or not); and any follow actions that were agreed to be carried out or passed to a colleague/third party for actioning.

3.23 **Records Management**

Records will be correctly indexed and at all times be stored securely, accessed only by colleagues as part of their work responsibilities, disposed of in accordance with the Document Retention and Disposal Schedule and be adequate, relevant and not excessive for their desired purpose.

Colleagues will ensure when creating or maintaining any documentation containing Personal Data (including colleague Personal Data), that they have a Lawful Basis such as Contract, Legitimate Interest or Consent in place to permit the Processing of that Personal Data for that purpose.

If Consent is the applicable Lawful Basis, the Data Subject does have the Right to remove or amend that Consent at any time – and this must be reflected by amendment or removal of the applicable Personal Data within the document without undue delay.

All colleagues have a responsibility to ensure that the Personal Data The Group processes about them is correct and they should take appropriate action to ensure it is accurate wherever they are aware it is being Processed.

Colleagues will ensure that when creating or deleting registers, libraries or anything else that contains a volume of information that it is recorded in, or removed from, the Information Asset Register and Assets and Liabilities Register as required.

3.24 **Responsibilities**

The Senior DPBP has overall responsibility for the day-to-day implementation of this policy as well as also being responsible for:

- Keeping the Board, Committees and Management Team updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and policies on a regular basis.
- Arranging data protection training and advice for all colleagues and those included in this policy.
- Answering questions on data protection from colleagues, Board/Committee/Management Team members and other Stakeholders.
- Responding to individuals such as clients and employees who wish to know what data is being held on them by Karbon Homes.
- Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing.

The Data Protection team must:

- offer guidance to colleagues to assist them in ensuring their activities do not fall foul of Data Protection and related legislation;
- manage breaches and Right requests in a timely manner; and
- provide assistance and guidance to colleagues on matters relating to information management and data protection.

The Director: ICT and Digital Transformation is responsible for:

- ensuring that all systems, services, software and equipment meet acceptable security standards.
- checking and scanning security hardware and software regularly to ensure it is functioning properly; and
- researching and approving third-party services, such as cloud services the company is considering using to store or process Data.

People & OD must:

- provide guidance and support relating to actions being undertaken due to misuse of this Policy and associated procedures, this may include formal action under the Disciplinary or Capability policies.

Line managers must ensure that their colleagues:

- are aware of, and work in adherence to, the Data Protection Policy and its associated procedures;
- record interactions with customers appropriately; and
- have completed all required data protection training in a timely manner.

All colleagues have a responsibility in ensuring that The Group fulfils its Data Protection requirements as well as:

- familiarising themselves with this policy and associated procedures and complying with their requirements;
- completing any mandatory Data Protection training without any undue delay;

- ensuring the Personal Data The Group processes about them and their family members is accurate and up to date;
- advising the Data Protection team of any information requests or Data Breaches;
- ensuring when required that ID verification is performed before information is shared; and
- only sharing information with others what is necessary for the performance of a task (data minimisation principle) and not sharing information without a lawful basis.

3.25 **Register of Processing Activities**

It is a mandatory requirement of Data Protection legislation that The Group documents its processing activities and for this purpose The Group maintains a Register of Processing Activities (ROPA).

This document is continuously updated by the Data Protection team in line with the activities of The Group and includes information about the Processing activity, the categories of Data Subject and types of Personal/Special Category data in scope, our lawful basis for the processing, its retention period, the systems that the processing occurs on and who it is externally shared with.

Colleagues should ensure that when amending an existing or bringing in any new processes or third-party involvement, that the data protection team is made aware so the ROPA can be amended accordingly.

3.26 **Right to Rectification**

A Data Subject has the right to expect us to correct inaccurate personal information that we may hold on them

A Data Subject may advise us that the personal information we process on them is incorrect and they have the right to expect us to correct this information without undue delay

3.27 **Right to be Forgotten / Right to Erasure**

A Data Subject may request that any information held on them is deleted or removed and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

3.28 **Special Category Data**

In most cases where we process special categories of personal data, we will require the Data Subject's explicit consent to do this unless exceptional circumstances apply, or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

3.29 **Subject Access Requests / Right of Access**

Please note that in accordance with Data Protection legislation, individuals are entitled, subject to certain exemptions, to request access to information held about them.

If you receive a subject access request, you should refer that request **immediately** to the Data Protection team as Data Protection legislation imposes strict deadlines on us to respond. We may ask you to help us comply with those requests.

Please contact the Data Protection team if you would like to request information that we hold about you. There are also restrictions on the information to which you are entitled under applicable law.

Further guidance on Subject Access Requests can be found in the Subject Access Request procedure.

3.30 **Supervisory Body**

The Group Supervisory body for Data Protection is the Information Commission(IC) – formerly the Information Commissioners Office (ICO).

Website: https://ico.org.uk

Phone: 0303 123 1113

Address: Information Commission, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

3.31 **Surveys**

All colleagues must ensure that when they intend to survey customers or Stakeholders that they have an appropriate Lawful Basis in place before carrying out the survey.

Further guidance on surveying can be found in the Customer and Stakeholder Survey procedure.

3.32 **Third party requests for information**

Whilst we want to assist wherever possible by supplying third parties with copies of the Personal Data we process about a Data Subject, we must always ensure that before any information is shared, we have a lawful basis in place to enable the sharing.

In emergency situations where a life is at risk, we can share limited Personal Data with a third party when we are comfortable and confident of who the third party is and why the information is needed.

Further guidance on managing third party requests for information can be found in the Verification procedure.

3.33 **Training**

All colleagues will receive mandatory online training on this policy and data protection. New joiners will receive training as part of the induction process with further training provided at least every three years or whenever there is a substantial change in our policy or procedures, the law, or if deemed necessary due to their involvement in a data breach or other data protection related activity.

3.34 **Transferring Data internationally**

There are restrictions on international transfers of Personal Data. You must not transfer Personal Data anywhere outside the UK without first consulting the Senior DPBP/DPIMC.

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:

- The country to which the Personal Data is transferred ensures an adequate level of protection for the Data Subjects' rights and freedoms.
- The Data Subject has given her/his consent.
- The transfer is necessary for one of the reasons set out in 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.
- The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.
- 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.

Subject to the requirements above, Personal Data we hold may also be processed by colleagues operating outside the EEA who work for us or for one of our suppliers. That colleagues may be engaged in, among other things, the fulfilment of contracts with the Data Subject, the Processing of payment details and the provision of support services.

3.35 **Further Information**

If you have any questions about this Policy, please contact a member of the Data Protection team at data.protection@karbonhomes.co.uk

Further information on Data Protection including accessing the associated Data Protection procedures can be found on the data protection area on Kore, additional training found online via our learning system.

4.0 Monitoring and Review

4.1 All colleagues must observe this policy and the Senior DPBP has overall responsibility for this policy. The Senior DPBP will monitor it regularly in collaboration with the Director of Governance to make sure it is being adhered to. The policy will be reviewed in accordance with changes in legislation, guidance, organisational change or best practice.

4.2 Performance will be reported to The Group Audit and Risk Committee on a quarterly basis. Further monitoring to our Karbon Management Team and Executive Team members is reported on a quarterly basis.

5.0 Equality, Diversity and Inclusion

5.1. This policy is applied in line with our Inclusion and Belonging Policy. This includes the legal requirements of the Equality Act 2010, Workers Protection Act 2023 and the Public Sector Equality Duty.

5.2. At Karbon we aim to eliminate discrimination, promote equality of opportunity, foster good relations and define the nine protected characteristics of age, disability, gender reassignment, marriage or civil partnership, pregnancy or maternity, race, religion or belief, sex, or sexual orientation.

5.3. If you would like this or any other policies in different language or format, please contact inclusion@karbonhomes.co.uk.

6.0 Changes to this Policy

6.1 We reserve the right to change this policy at any time. Where appropriate, we will notify you and any Data Subjects of those changes by email.

7.0 Data Protection and Privacy

7.1 We take compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our Disciplinary Policy which may result in dismissal.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the Senior DPBP.