Group Data Protection Policy

1. Introduction

1.1 This Group Data Protection Policy sets out how Coastline (Coastline Housing Limited and group companies) will handle the personal data of its customers, suppliers, employees, workers and other third parties.

1.2 Coastline is committed to a policy of protecting the rights and privacy of individuals in accordance with the General Data Protection Regulations (GDPR) and Data Protection Legislation.

1.3 The Data Protection Legislation lays down regulations and safeguards for the collection, recording and use of personal information whether on paper, in a computer or recorded on other material. Coastline needs to collect and use certain types of information about people with whom it deals in order to operate. These include employees, employment applicants, customers, housing applicants, Non-Executive Directors (NEDs), suppliers and others with whom it communicates.

1.4 Certain information may be required for regulatory or monitoring purposes as laid down by statute. Other information may be required for the purpose of establishing a contract. In any case, Coastline recognises that the information must be dealt with lawfully and correctly under the principles laid down within legislation.

2. Key Definitions

2.1 **Automated decision making** (ADM) – when a decision is made based solely on automated processing (including profiling) which produces legal effects or significantly affects an individual.

2.2 **Coastline** – Coastline Housing Limited and group companies.

2.3 **Data Controller** – the person or organisation that determines when, why and how to process Personal data. It is responsible for establishing practices and policies in line with the GDPR. Coastline is therefore the Data Controller of all personal data used in its business activities.

2.4 **Data Privacy Impact Assessment** (DPIA) – assessments used to identify and reduce risks of data processing activity, and should be conducted for all major system or business change programmes involving the processing of personal data.

2.5 **Data Processing Agreement** – agreement between Coastline and third party confirming that processing of personal data safeguards are in place.

2.6 **Data Processor** – the organisation performing activities as required by the Data Controller.

2.7 **Data Protection Officer** (DPO) – the person with responsibility for Data Protection compliance.

2.8 **Data Subject** – a living, identified or identifiable individual about whom personal data is held.

2.9 **EEA** – currently the 27 countries in the European Union plus Iceland, Norway, Liechtenstein and UK.

2.10 **Employees** – staff, NEDs, agency staff, temps, consultants and volunteers undertaking Coastline business activities.

2.11 **Information Asset Register** (IAR) – internal document which registers the nature of information held, location, format and accessibility, responsible manager, who the information is shared with, the purpose and the basis for holding the information (legal, contractual, consent or legitimate business interest).

2.12 **Information Commissioners Office** (ICO) - is the supervisory body for Data Protection in the UK.

2.13 **Personal data** – any information relating to an identified or identifiable natural person. This is someone who can be identified directly or indirectly by reference to an identifier such as a name, identification number, location data or online identifier of that natural person.

2.14 **Privacy by Design** – implementing appropriate technical and organisational measures in an effective manner to ensure compliance with GDPR.

2.15 **Privacy Notice** (sometimes referred to as Fair Processing Notices) – separate notices setting out information which may be provided to Data subjects when information is collected about them. These notices may take the form of general privacy statements applicable to a specific group of

individuals (for example employee privacy notices or the website privacy notice) or they may be stand-alone statements covering processing related to a specific purpose.

2.16 **Sensitive personal data** – information revealing racial or ethnic origin, political opinion, religious or similar beliefs trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data and Personal Data relating to criminal offenses and convictions.

3. Scope

3.1 This Policy applies to all personal data processed regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

3.2 This Policy applies to all Coastline employees who must read, understand and comply with this Policy when processing Personal data on Coastline's behalf and attend training on its requirements. This Policy sets out what is expected in order for Coastline to comply with applicable law and compliance with this Policy is mandatory. Related Policies and guidance are available to help interpret and act in accordance with this Policy and breach of this Policy may result in disciplinary action.

3.3 All individuals are responsible for ensuring compliance with this Policy and implement appropriate practices, processes, controls and training to ensure such compliance.

3.4 Coastline has appointed the Company Secretary as its Data Protection Officer. The responsibilities of this role include;

- Informing and advising Coastline and its employees about data protection requirements.
- Monitoring compliance with data protection laws and Coastline policies including managing internal data protection activities, ensuring that staff are trained and conducting audits.
- Providing advice on data protection impact assessments and monitoring impact assessment performance.
- Co-operating with and acting as a point of contact for the ICO.

4. Personal data protection principles

4.1 Coastline adheres to the principles relating to processing of Personal data set out in the GDPR which require Personal data to be:

(a) Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).

(b) Collected only for specified, explicit and legitimate purposes.

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (known as Data Minimisation).

(d) Accurate and where necessary kept up to date.

(e) Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is processed.

(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

(g) Not transferred to another country without appropriate safeguards being in place.

(h) Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal data (Data Subject's Rights and Requests).

4.2 Coastline is responsible for and must be able to demonstrate compliance with the data protection principles listed above.

5. Lawfulness, fairness, transparency

5.1 Lawfulness and fairness

5.1.1 Personal data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

5.1.2 You may only collect, process and share Personal data fairly and lawfully and for specified purposes. The GDPR restricts actions regarding Personal data to specified lawful purposes. These restrictions are not intended to prevent processing, but ensure that Personal data is processed fairly and without adversely affecting the Data Subject.

5.1.3 The GDPR allows Processing for specific purposes, some of which are set out below:

(a) the Data Subject has given his or her Consent;

(b) the Processing is necessary for the performance of a contract with the Data Subject;

(c) to meet legal compliance obligations.;

(d) to protect the Data Subject's vital interests; or

(e) to pursue our legitimate interests for purposes where they are not overridden because the processing prejudices the interest or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal data for legitimate interests need to be set out in applicable Privacy Notices or Fair Processing Notices.

5.1.4 Coastline identifies in the Information Asset Register the legal ground being relied on for each processing activity in accordance with the requirements on lawful basis for processing Personal data.

5.2 Lawful basis for processing

5.2.1 A Data Controller must only process Personal data on the basis of one or more of the lawful bases set out in the GDPR, which includes consent, legal, contractual or legitimate business interests.

5.2.2 Most processing of personal data will be undertaken because Coastline has either a legal, contractual or legitimate business interest to do so. For example, it is a legal requirement to report an accident under Health and Safety legislation; a contractual requirement to deal with matters under the Tenancy Agreement; or a legitimate business interest to hold emergency contact details for a member of staff. Coastline maintains full details in the Information Asset Register (see 5.1.4).

5.2.3 Where specific consent is needed a Data Subject consents to processing of their Personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

5.2.4 Data Subjects must be easily able to withdraw Consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to process Personal data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

5.2.5 Unless relying on another legal basis for processing, explicit Consent is usually required for processing Sensitive Personal data and for Automated Decision-Making (ADM). Usually Coastline will be relying on another basis (and not require explicit Consent) to process most types of Sensitive Data. Where explicit Consent is required, you must issue a Privacy Notice to the Data Subject to capture explicit Consent.

5.2.6 Coastline must evidence Consent captured and keep records of all Consents so that compliance can be demonstrated.

5.3 Transparency (notifying data subjects)

5.3.1 The GDPR requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

5.3.2 Whenever Personal data is collected directly from Data Subjects, including for Human Resources or employment purposes, the Data Subject must be provided with the information required by the GDPR including the identity of the Data Controller, the DPO, how and why the information will be used, protected and retained.

5.3.3 When Personal data is collected indirectly (for example, from a third party or publically available source), the Data Subject should be provided with all the information required by the GDPR as soon as possible after collecting the data.

5.3.4 In most instances the Privacy Notice made available in hard copy or on the website will give sufficient detail for the purpose of routine data processing.

6. Purpose limitation

6.1 Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

6.2 It is not permissible to use Personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless the Data Subject has been informed of the new purposes and Consent has been given or an alternative processing basis determined.

7. Data minimisation

7.1 Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

7.2 Adequate Personal data may only be collected for the purpose intended.

7.3 When Personal data is no longer needed for the specified purpose it must be deleted or anonymised in accordance with the Document Retention Policy (*Document retention policy* **).**

8. Accuracy

8.1 Personal data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

8.2 Coastline will ensure that Personal data held will be accurate, complete, kept up-to-date and relevant for the purpose for which it was collected. All reasonable steps must be taken to destroy or amend inaccurate or out-of-date Personal data.

9. Storage limitation

9.1 Personal data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

9.2 Personal data must not be kept in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which the data was originally collected.

9.3 Coastline will maintain retention policies and procedures to ensure Personal data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time (*Document retention policy*).

9.4 Coastline will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

10. Security integrity and confidentiality

10.1 Protecting Personal data

10.1.1 Personal data must be secured by appropriate measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

10.1.2 Coastline will develop, implement and maintain safeguards appropriate to its size, scope and business, available resources and the amount of Personal data that is held or maintained on behalf of others.

10.1.3 Employees must follow all procedures in place to maintain the security of all Personal data from the point of collection to the point of destruction. Personal data may only be transferred to third-party service providers who agree to comply with the required policies and procedures (Data Processing Agreements) and who agree to put adequate measures in place, as requested.

10.1.4 Employees must maintain data security by protecting the confidentiality, integrity and availability of the Personal data, defined as follows:

(a) Confidentiality means that only people who have a need to know and are authorised to use the Personal data can access it.

(b) Integrity means that Personal data is accurate and suitable for the purpose for which it is processed.

(c) Availability means that authorised users are able to access the Personal data when needed for legitimate authorised purposes.

10.1.5 There are a range of security measures at Coastline's offices designed to prevent unauthorised access, including access controls and CCTV (*CCTV Policy*).

10.1.6 Whilst much of Coastline's personal data is held electronically, some data will also be in hard copy. In the interests of confidentiality and security of information, employees must ensure that they clear their desk of personal data at the end of every day.

10.1.7 The IT Acceptable Use Policy outlines 'acceptable usage' for various aspects of IT equipment and services with a focus on the security and protection of systems and data. It includes mobile devices, personal devices and remote working.

10.2 Reporting a Personal data Breach

10.2.1 Coastline has in place policy and procedures to deal with any suspected Personal data breach and will notify Data Subjects or any applicable regulator where it is legally required to do so (*Guidance on Data Breach Management*).

10.2.2 Any breach where it is likely to result in a risk to the rights and freedoms of individuals will be reported to the ICO. Coastline will do this within the required 72 hours' time period of Coastline becoming aware of the breach.

10.2.3 In addition Data protection breaches will be reported to the Chair of the Audit, Assurance & Risk Committee and to the next scheduled Committee meeting.

11. Transfer limitation

11.1 The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined.

11.2 Personal data may only be transferred outside the EEA if one of the following conditions applies:

(a) the European Commission has issued a decision confirming that the country to which we transfer the Personal data ensures an adequate level of protection for the Data Subjects' rights and freedoms;

(b) appropriate safeguards are in place such as binding corporate rules, standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;

(c) the Data Subject has provided explicit Consent to the proposed transfer after being informed of any potential risks; or

(d) the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract Coastline and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

12. Data Subject's rights and requests

12.1 Data Subjects have rights when it comes to how their Personal data is handled. These include rights to:

(a) withdraw Consent to processing at any time;

(b) receive certain information about the Data Controller's processing activities;

(c) request access to their Personal data;

(d) prevent use of their Personal data for direct marketing purposes;

(e) to erase Personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;

(f) restrict processing in specific circumstances;

(g) challenge processing which has been justified on the basis of our legitimate interests or in the public interest;

(h) request a copy of an agreement under which Personal data is transferred outside of the EEA;

(i) object to decisions based solely on Automated Processing, including profiling (ADM);

(j) prevent processing that is likely to cause damage or distress to the Data Subject or anyone else;

(k) be notified of a Personal data Breach which is likely to result in high risk to their rights and freedoms;

(l) make a complaint to the supervisory authority; and

(m) in limited circumstances, receive or ask for their Personal data to be transferred to a third party in a structured, commonly used and machine readable format.

12.2 The identity of an individual requesting data must be verified (eg photo identification) when requesting data under any of the rights listed above.

12.3 You must immediately forward any Data Subject Access Request (SAR) received to the DPO or their nominated deputy, the Assistant Company Secretary.

13. Accountability

13.1 The Data Controller must implement appropriate measures in an effective manner, to ensure compliance with data protection principles. The Data Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

13.2 Coastline must have adequate resources and controls in place to ensure and to document GDPR compliance including:

(a) appointing a suitably qualified DPO accountable for data privacy;

(b) implementing Privacy by Design when processing Personal data and completing DPIAs where processing presents a high risk to rights and freedoms of Data Subjects;

(c) integrating data protection into internal documents including this Policy, related policies or Privacy Notices.

(d) regularly training employees on the GDPR, this Policy and related policies and data protection matters including, for example, Data Subject's rights, Consent,

legal basis, DPIA and Personal data Breaches. Coastline must maintain a record of training attendance; and

(e) conduct periodic reviews and audits to assess compliance.

14. Record keeping

14.1 Coastline is required to keep full and accurate records of all data processing activities.

14.2 Records should include at a minimum, the name and contact details of the Data Controller and the DPO, clear descriptions of the Personal data types, Data Subject types, processing activities, processing purposes, third-party recipients of the Personal data, Personal data storage locations, Personal data transfers, the Personal data's retention period and a description of the security measures in place.

14.3 An Information Asset Register (IAR) has been produced and maintained by relevant identified senior managers responsible for the service which is collecting and or managing the data.

15. Training and audit

15.1 Coastline requires all employees to undertaken mandatory training to enable them to comply with data privacy laws.

15.2 Coastline will regularly review all the systems and processes under its control to ensure they comply with this Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal data.

16 Privacy By Design and Data Protection Impact Assessment (DPIA)

16.1 Coastline is required to implement Privacy by Design measures when Processing Personal data by implementing appropriate measures in an effective manner, to ensure compliance with data privacy principles.

16.2 Managers must assess what Privacy by Design measures can be implemented on all new or high risk programs/systems/processes that process Personal data by taking into account the following:

(a) the state of the art;

(b) the cost of implementation;

(c) the nature, scope, context and purposes of Processing; and

(d) the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the processing.

(e) a description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate;

(f) an assessment of the necessity and proportionality of the Processing in relation to its purpose;

(g) an assessment of the risk to individuals; and

(h) the risk mitigation measures in place and demonstration of compliance.

17. Automated Processing (including profiling) and Automated Decision-Making

17.1 Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

(a) a Data Subject has explicitly Consented;

(b) the processing is authorised by law; or

(c) the processing is necessary for the performance of or entering into a contract.

17.2 If certain types of Sensitive Data are being processed, then grounds (b) or (c) will not be allowed but such Sensitive Data can be Processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

17.3 Whilst Coastline does not use ADM, should it arise then a DPIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

18. Direct marketing

18.1 Coastline has only limited direct marketing activities however under GDPR is subject to certain rules and privacy laws when marketing to our customers.

18.2 For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

18.3 The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

18.4 A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

19. Sharing Personal data

19.1 Generally it is not allowed to share Personal data with third parties unless certain safeguards and contractual arrangements have been put in place.

19.2 Personal data may only be shared with another employee, contractor, agent or representative of the Group (which includes subsidiaries) if the recipient has a job-related need to know the information.

19.3 Personal data may only be shared with third parties, such as service providers if:

(a) they have a need to know the information for the purposes of providing the contracted services;

(b) sharing the Personal data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

(c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place; and

(d) a fully executed written contract that contains GDPR approved third party clauses has been obtained.

20. Policy Review

20.1 This Policy will be monitored to ensure it meets good practice and will be reviewed by the Audit, Risk & Assurance Committee every three years or earlier should any significant changes arise.

21. Related Policies and Procedures

Guidance on Data Security Breach Management

Data Retention Policy

CCTV Policy

Privacy Impact Assessments

Privacy Notice