Data Protection Policy

Policy information	
Organisation	Data Controller: Claybournes "data controller" means an entity which (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed
Scope of policy	This policy applies to the Claybournes only. Registered Address: Unit 7, Cherry Holt Square, Bourne PE10 9LA The company has no data processors. "data processor", in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.
Policy operational date	Operational Date: 25/05/2018
Policy prepared by	Prepared by Michael McDonald on behalf of Claybourne's DPO: Jason Brooke.
Date approved	Approved: 21/05/2018
Policy review date	Review Date: 25/05/2021

Introduction	
Purpose of policy	This policy was prepared for the following purposes: • complying with General Data Protection Regulation 2018 (GDPR) • follow good practice • protect clients, staff and other individuals • protect the organisation
Types of data	• Personal data relating to suppliers and consumers is stored strictly for the purposes of receiving and fulfilling orders through goods and/or services. • Personal data received from inquiries for good and/or services made by phone, web form and email. • Data relating to staff is stored for HR and recruitment purposes.
Policy statement	Claybournes is committed to: • complying with both the law and good practice • respecting individuals' rights • being open and honest with individuals whose data is held • providing training and support for staff who handle personal data, so that they can act confidently and consistently • notify the Information Commissioner voluntarily, even if this is not required
Key risks	This should identify the main risks within your organisation in two key areas: • data getting into the wrong hands, through poor security or inappropriate disclosure of information • individuals being harmed through data being inaccurate or insufficient

Responsibilities	
The Board / Company Directors	They have overall responsibility for ensuring that the organisation complies with its legal obligations.
Data Protection Officer	Responsibilities include: • Briefing the co-owners on Data Protection responsibilities • Reviewing Data Protection and related policies • Advising other staff on tricky Data Protection issues • Ensuring that Data Protection induction and training takes place • Notification to the ICO • Handling subject access requests • Approving unusual or controversial disclosures of personal data • Approving contracts with Data Processors
Employees & Volunteers	All staff are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work.
Enforcement	All staff are required to receive data protection training and refreshers on an annual basis. Staff found not to be complying will be reprimanded and provided further training.

Security	
Scope	Data Security specifically applicable to Data Protection.
Setting security levels	The consequences of a breach of confidentiality are dependant on proven intent and size and scale of breach.
Security measures	• The DPO will ensure that Data Protection induction and training takes place. • Specific training regarding phishing will be provided to all employees. • All devices containing personal data will be password protected. The password will not be shared with anyone but the owner. • PCs and mobile devices will be subject to automatic idle log outs. • All devices will have up-to-date virus protection. • All paper documentation will be securely stored until such time it is destroyed. • Social media marketing will be restricted to standard social channel protocols (currently only Facebook). • Emails older than five year will be deleted on a monthly basis. • No physical backups of any personal data will be created. • All staff information will be destroyed 6 months following their leaving date. • Any CVs will be destroyed immediately after position is filled unless permission provided to store for a longer set period. • This policy will be reviewed and re-issued if 'non-social media' marketing operations commence. • If marketing operations commence; explicit consent will be sought. • The website: www.claybournes.co.uk; does not and will not store personal data relating to anyone. • The most up-to-date policy will be available at www.claybournes.co.uk.
Specific risks	• Information taken illegitimately (such as phishing) via email, phone or face-to-face. • Personal information sent to third party in error. • Trojan type virus on company PCs transmitting information to a third party.

Data recording and storage	
Accuracy	Information accuracy is ensured by: • Confirming with the individual when receiving information over the phone. • If suspected incorrect; the individual is contacted through their preferred method of communication.
Updating	Unless express permission is provided by the individual; all records containing personal information relating to customers and/or suppliers will be destroyed after 5 years following fulfilment of goods and/or services. Unless express permission is provided; all information relating to staff or recruitment will be destroyed following 6 months of terminations or application.
Storage	All data will be stored securely. Paper based data will be physically locked away and all computer based data will be password protected in accordance with best practice.
Retention periods	Unless express permission is provided by the individual; all records containing personal information relating to customers and/or suppliers will be destroyed after 5 years following fulfilment of goods and/or services. Unless express permission is provided; all information relating to staff or recruitment will be destroyed following 6 months of terminations or application.
Archiving	All data outside of the specific retention policy timescales will be destroyed. Paper-based data will be shredded and PC based data will be deleted.

Right of Access	
Responsibility	Right of access requests will be handled within the legal time limit which is one month from receiving the request.
Procedure for making request	Right of access requests must be in writing. All employees are responsible for passing on anything which might be a subject access request to the DPO without delay.
Provision for verifying identity	Where the DPO managing the access procedure does not know the individual personally identification will be requested.
Charging	Claybournes will charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive. Claybournes may also charge a reasonable fee to comply with requests for further copies of the same information. This does not mean the requester will be charged for all subsequent access requests. The fee will be based on the administrative cost of providing the information. Please contact the ICO for further information regarding consumer rights in regard to Data Protection.
Procedure for granting access	If the request is made electronically, Claybournes will provide the information in a commonly used electronic format (e.g. .pdf, .doc, .xls, etc).

Transparency	
Commitment	Claybournes is committed to ensuring that Data Subjects are aware what data is being processed and • for what purpose it is being processed • what types of disclosure are likely, and • how to exercise their rights in relation to the data
Procedure	Data Subjects are informed using the following methods: • employees briefed on commencement of employment • suppliers and consumers informed via email, over the phone or face-to-face
Responsibility	The data protection officer is responsible for ensuring compliance with this policy.

Lawful Basis	
Underlying principles	Claybournes stores personal data under lawful basis dependant on circumstances: • Consent: the individual has given clear consent for you to process their personal data for a specific purpose. • Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract. • Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
Opting out	Claybournes will consider giving individuals the opportunity to opt out of their data being used in particular ways.
Withdrawing consent	Claybournes acknowledge that, once given, consent can be withdrawn, but not retrospectively. There may be occasions where Claybournes has no choice but to retain data for a certain length of time, even though consent for using it has been withdrawn.

Employee training & Acceptance of responsibilities	
Induction	All employees who have access to any kind of personal data have their responsibilities outlined during their induction procedures.
Continuing training	Opportunities to raise Data Protection issues during employee training are provided and welcomed.
Procedure for staff signifying acceptance of policy	All employees confirm understanding and acceptance of their responsibilities to Data Protection. This policy is available at www.claybournes.co.uk.

Policy review	
Responsibility	The DPO is responsible for reviewing this policy and associated procedures.
Timing	This policy is reviewed every three years.

For more information, please visit the ICO website: www.ico.org.uk