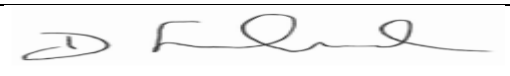
DATA PROTECTION

POLICY

Policy Lead	**Mike Cairns** **(Head of Finance and IT)**
Policy Author	**Mike Cairns** **(Head of Finance and IT)**
Department / **Policy Reference Number /** **Policy Version**	**6.1.6** **6 = IT & DPA** **1 = Policy Reference Number** **6 = 2021**
Policy Effective Date	**June 2021**
Policy Review Date	**June 2022** (or as and when statutory / legislative changes)
Board Approval Date	**June 2021**
Board Member Signature	
Dissemination to employees (Method and Date)	New starters – Core Induction / Read and Sign File. Current Employees – Read and Sign File / Supervision

Contents

Policy Section

Appendices

1. Dealing with Data Breaches

POLICY SECTION

1. Policy Statement

1.1 Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities Halliwell Homes Limited (we) will collect, store and process personal data about our residents, employees, workers, visitors, suppliers and other third parties, and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

1.2 We regard the lawful and correct treatment of personal information as very important to the successful and efficient performance of our business and to the maintenance of confidence between those with whom we deal. Protecting the confidentiality and integrity of personal data is a critical responsibility that we take seriously at all times. To this end we have devised and regularly update policies on how personal data is to be processed by us, those who we work for and (to the extent that they are the data processors) those who work with us.

1.3 Data users (as defined below) are obliged to comply with this policy when processing personal data on our behalf. Any breach of this policy by an employee or worker may result in disciplinary action.

2. About This Policy

2.1 The types of personal data that we may be required to handle include information about current and past and residents, contractors, applicants for jobs, employees, workers, local authority contacts and others that we communicate with. The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 2018 (the Act), the General Data Protection Regulation (EU) 2016/679 (GDPR) and other regulations and codes of practice.

2.2 This policy and any other documents referred to in it sets out the basis on which we will process any personal data we collect from individuals, or that is provided to us by those individuals or others (including our customers, suppliers, employees and workers).

2.3 This policy does not form part of any employee or worker's contract of employment or service and may be amended at any time

2.4 This policy has been approved by the board of directors. It sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data. It applies to all personal data that we process regardless of the media on which that data is stored

2.5 The Data Protection Compliance Manager is responsible for ensuring compliance with the Act and with this policy. That post is held by Mike Cairns (Head of Finance & IT) 0161 437 9491, mike.cairns@halliwellhomes.co.uk. 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 Compliance Manager

2.6 All of our employees have undertaken training on data privacy.

3. Definition of Data Protection Terms

3.1 Data is information which is stored electronically, on a computer, or in certain paper-based filing systems.

3.2 Data controllers are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Act. We are the data controller of all personal data used in our business for our own commercial purposes.

3.3 Data processors are persons or organisations that is not a data user that processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition, but it could include suppliers which handle personal data on our behalf

3.4 Data subjects, for the purpose of this policy, include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

3.5 Data users are those of our employees or workers 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.

3.6 Personal data is subject to the legal safeguards specified in the GDPR and the Act.

3.7 Personal data means data relating to a living individual who can be identified from that data (or from that data alone or in combination with other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

3.8 Processing is any activity that involves use of personal data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

3.9 Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, 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

4. Data Protection Principles

Anyone processing personal data must comply with the following principles of good practice. These provide that personal data must be:

Lawfulness, fairness and transparency	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.
Purpose limitation	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
Data minimisation	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
Accuracy	Personal data shall be accurate and, where necessary, kept up to date.
Storage limitation	Personal data shall be kept in a form which permits identification of the data subject for no longer than is necessary for the purpose for which the personal data is processed.
Security, Integrity and confidentiality	Personal data shall be 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.
Accountability	The controller shall be responsible for and be able to demonstrate compliance with applicable data protection law.

Transfer Limitation	Personal data must not be transferred to another country without appropriate safeguards in place.
Data Subject's Rights and Requests	Personal data must be made available to data subjects and data subjects are allowed to exercise certain rights in relation to their personal data.

5. Lawfulness, Fairness and Transparency

5.1 The Act is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

5.2 For personal data to be processed lawfully, they must be processed on the basis of one of the following legal grounds:

(a) the data subject consents to the processing;

(b) the processing is necessary for:

(i) performing the contract with a data subject;

(ii) complying with a legal obligation;

(iii) protecting the vital interests of the data subject for performing a task carried out in the public interest; or

(iv) pursuing the legitimate interest of the data controller or a third party (except where the data subject's interests, or fundamental rights and freedoms override the data controller's interest).

6. Processing for Limited Purposes

6.1 In the course of our business, we may collect and process the personal data set out in Schedule 1. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, business partners, sub-contractors in technical, payment and delivery services and others).

6.2 We will only process personal data for the specific purposes set out in the Schedule 1 or for any other purposes specifically permitted by the Act. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

Notification will normally take the form of making the data subject aware of our privacy policy, but we may provide specific privacy notices in some cases.

7. Notifying Data Subjects

7.1 If we collect personal data directly from data subjects, we will inform them about:

(a) The purpose or purposes for which we intend to process that personal data.

(b) The types of third parties, if any, with which we will share or to which we will disclose that personal data.

(c) The means, if any, with which data subjects can limit our use and disclosure of their personal data.

(d) How long we will keep their data for.

(e) The rights the data subject has in relation to the personal data we hold.

7.2 If we receive personal data about a data subject from other sources, we will provide the data subject with this information as soon as possible thereafter.

7.3 Where appropriate, we will also inform data subjects whose personal data we process that we are the data controller with regard to that data.

7.4 We openly publish our privacy policy and refer to it wherever we collect personal data and endeavour to keep the privacy policy as up to date as possible.

However, where data subjects have specific questions about how their personal data is handled, we will always be open and transparent with them and as clear as possible when dealing with their enquiries.

8. Adequate, Relevant and Non-Excessive Processing

8.1 We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

8.2 When personal data is no longer needed for specified purposes we will delete or anonymise it in accordance with this policy.

8.3 Employees or workers must only process personal data when performing their job duties requires it.

9. Accurate Data

We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data in particular we will promptly update any personal data which we are notified by a data subject is not accurate or up to date.

10. Timely Processing

10.1 We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy or erase from our systems (where it is technically possible to do so), all data which is no longer required. Where applicable, we will request third parties delete such data.

10.2 We have developed, and regularly review, a data retention policy for the different types of personal data that we process, and this is as follows:

Type of Personal Data	Retention Period
Personal data of employees or workers	For 6 years after the employee or worker leaves employment or service.
Personal data in relation to unsuccessful job applicants	Personal data retained for up to 6 months following the filling of the position for which they applied.
Personal data in relation to children in our care	Until the 75th anniversary of the child's birth or, if the child dies before age 18, for 15 years from the date of death as dictated by the Children's Homes (England) Regulations 2015. (Regulation 36)
Personal data in relation to data subjects on our marketing data base	The personal data is kept until such time as the data subject notifies us that they no longer wish to receive correspondence from us which they may do at any time.
Data concerning suppliers to the business	As long as is reasonably necessary in order to perform any contract with such suppliers and as is necessary for legal or accounting purpose thereafter.

11. Processing in Line with Data Subject's Rights

11.1 We will process all personal data in line with data subjects' rights, in particular their right to:

(a) Request access to any data held about them by a data controller (see also Clause 16).

(b) Prevent the processing of their data for direct-marketing purposes.

(c) Ask to have inaccurate data amended (see also Clause 9).

(d) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

(e) Have data erased (see Clause 18).

(f) Withhold consent to processing at any time (if it is processed on the basis of consent).

12. Collection and Use of Sensitive Personal Data

Given the nature of our business we will, inevitably, collect some sensitive personal data. This information is stored with the upmost security and it can only be accessed on a strictly "need to know" basis.

13. Data Security

13.1 We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. We regularly test our systems and processes to assess compliance.

13.2 We have 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 will only be transferred to a data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself and only if the data processor has entered into a formal contract with us.

13.3 We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

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

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

(c) 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 the company's central computer system instead of individual PCs.

13.4 Security procedures include:

(a) Entry controls. Any stranger seen in entry-controlled areas should be reported.

(b) 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.)

(c) Methods of disposal. Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.

(d) 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.

(e) Clear desks. Data users must ensure that, when they are absent from their desk, the desk is clear of all paperwork which may contain personal data.

(f) Download policy. No member of staff is entitled to download any software onto any device issued by the business or used in the course of business without the prior consent of the Head of IT.

14. Transferring Personal Data to a Country Outside the EEA

14.1 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:

(a) The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms.

(b) The data subject has given his consent.

(c) The transfer is necessary for one of the reasons set out in the Act, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject.

(d) The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.

(e) 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.

14.2 Subject to the requirements in Clause 14.1 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. This would only be done in the most exceptional of circumstances where a senior member of staff was travelling (whether for personal reasons or on business) and was required to access our systems.

15. Disclosure and Sharing of Personal Information

15.1 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.

15.2 We may also disclose personal data we hold to third parties:

(a) In the event that we sell or buy any business or assets, in which case we may disclose personal data we hold to the prospective seller or buyer of such business or assets.

(b) If we or substantially all of our assets are acquired by a third party, in which case personal data we hold will be one of the transferred assets.

15.3 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 and workers, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

15.4 We may also share personal data we hold with selected third parties for the purposes set out in the Schedule 1.

16. Dealing with Subject Access Requests

16.1 Data subjects may make a request for information we hold about them in writing or verbally. =. Any staff who receives a request (whether written or verbal) should forward it to the Data Protection Compliance Manager immediately.

16.2 When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:

(a) We will check the caller's identity to make sure that information is only given to a person who is entitled to it.

(b) We will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

16.3 Our staff will refer a request to the Data Protection Compliance Manager for assistance in all circumstances. Staff should not be bullied into disclosing personal information.

17. Dealing with Data Breaches

17.1 If you are aware of any breach or potential breach of this policy or data protection law generally you must inform the Data Protection Compliance Manager immediately. Please also see Appendix 1. If the Data Protection Compliance Manager is not available please contact David Sheffield on 0161 437 9491 or david.sheffield@halliwellhomes.co.uk. It does not matter how minor the breach or potential breach is, or even if you are unsure if there is a breach, please report every instance.

17.2 In the event that a breach is reported and verified of a breach of the law then we will report this to the Information Commissioner's Office (ICO) as soon as reasonably possible and within 72 hours of becoming aware of the breach. We will take all reasonable actions to mitigate the impact of the breach on data subjects (including informing data subjects of the breach if that is required).

17.3 Following a breach we will conduct a full review of the circumstances of the breach and make recommendations (and implement those recommendations) for improved policies, procedures, training or other actions which will be to better practice and minimise the chances of a similar breach occurring in the future.

18. Erasure of Personal Data

18.1 We endeavour to ensure that all personal data that's held in a physical format is either destroyed by us on site or is destroyed by a reputable company operating under a robust contract with us.

18.2 We conduct a "sweep" of our employee, worker and job applicant data approximately three times per year to ensure that data which we should no longer be keeping in accordance with our retention policy is erased.

18.3 We respect a data subject's "rights to be forgotten" but are under legal constraints in relation to information held about children, employees and workers which means that, in the majority of circumstances, their personal data must be retained for us in accordance with our retention periods.

19. Changes to This Policy

We reserve the right to change this policy at any time. Where appropriate, we will notify data subjects of those changes by mail or email.

Schedule 1 Data Processing Activities

Category of data subject	Types of personal data processed	Purpose for processing
Residents of our homes	Full name contact telephone number, date of birth, gender, next of kin contact details, medical/health conditions, bank account number, dietary requirements, medical history, history of abuse, copies of social work records and reports.	Necessary for our legitimate interests (to provide residential care). To comply with our legal obligations.
Suppliers	Contact names, address, contact telephone numbers and email addresses.	Necessary for our legitimate interests (for running our business). To comply with our legal obligations (and for any accountancy purposes).
Employees, workers, consultants, agents acting on our behalf	Full name, identity documents (such as passports and driving licences), address, bank account details, email address, date of birth, contact telephone number, next of kin details, criminal records information, sickness records, disciplinary records (where applicable), performance reviews, job title	Performance of a contract To comply with our legal obligations
Visitors to our homes	Full name, details of who they are visiting, vehicle registration if they have parked at our care home	Necessary for our legitimate interests (to protect the security of our homes and anyone staying at or visiting our homes). To comply with our legal obligations.
Third parties, such as local authority contacts that we work with	Contact name, email address, contact telephone number, job title	Performance of a contract and to comply with our legal obligations

Third parties that we customarily share personal data with

- Service providers who provide IT and system administration services.
- Professional advisers including lawyers, bankers, auditors and insurers, who provide consultancy, banking, legal, insurance and accounting services.
- HM Revenue & Customs, regulators and other authorities who require reporting of processing activities in certain circumstances.
- Email systems such as Mail Chimp.
- Electronic storage and transfer system such as Dropbox and Google Drive.

Appendix 1

Dealing with Data Breaches