

CHISLEHURST AND SIDCUP HOUSING ASSOCIATION PRIVACY POLICY

1.0 INTRODUCTION

- 1.1 The General Data Protection Regulation (GDPR) is the principal regulation, which makes provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. In accordance with the General Data Protection Regulations, the Association has put in place this Privacy Policy.
- 1.2 Chislehurst and Sidcup Housing Association (the Association) is a Registered Provider and is regulated by the Regulator of Social Housing. We provide social housing and support to individuals. The Association is the controller of information and decides the manner and purpose of how personal information is processed. The appointed Data Protection Officer for the Association is the Chief Executive and can be contacted at csinfo@cscha.org.uk, alternatively on 0208 467 9146.
- 1.3 The Association processes personal information from you when you register with us or contact us; or if you provide a service on our behalf. Processing of information means any information that we collect, edit, retain and store, disclose or share, delete/erase and destroy, view (including CCTV images) or listen to or archive.
- 1.4 Personal information relates to a living individual who can be identified, contacted or located by the information alone or together with other information. In essence any information relating to an identified or identifiable natural person who can be directly or indirectly identified in particular by reference to an identifier. Examples of personal information include name, address, dates of birth, bank details. Personal information may be stored electronically (including CCTV images) or as part of the Association's manual records.
- 1.5 The Association may also process sensitive personal information. This information can only be processed in certain circumstances. As the information is sensitive we will seek your consent to processing this type of information. It will depend on the relationship we have with you whether or not we process sensitive personal information. Examples of sensitive information include:-
- Racial or ethnic origin.
 - Political opinions.
 - Religious or philosophical beliefs.
 - Trade union membership.
 - Physical/mental health or condition.

- Sexual life or sexual orientation.
 - Genetic data.
 - Biometric data.
 - Commission or allegation of an offence.
 - Proceedings for any offence, disposal of proceedings or sentence.
- 1.6 We will only process personal information when we need it. The type of information we need from you will vary depending on our relationship with you. When we ask you for information, we will make it clear why we need it. We will also make it clear when you do not have to provide us with information and any consequences of not providing it. Most information we hold will be collected from you but we may also obtain this from third parties such as local authorities, doctors, health professionals, previous landlords, banks, and trade contractors, people you may have provided a service to before, people you have previously worked with or other relevant community partner or agency.
- 1.7 This policy applies to Tenants, Staff, Board Members, Contractors, Suppliers, service users. In essence it applies to personal information that we process about any individual. Any individual whose personal information is processed by the Association is known as a Data Subject. Therefore Data Subjects are Tenants, Ex Tenants, Contractors, Consultants, Suppliers, Staff, Board Members, relatives of Tenants.

2.0 PURPOSE

- 2.1 The purpose of this policy to explain to Data Subjects, how we as an organisation handle personal information. The legal basis for collecting such information, how it will be used, who it will be shared with, and the length of time information will be retained, how to access personal information and the rights that Data Subjects have.

3.0 PRINCIPLES OF THE GENERAL DATA PROTECTION REGULATION (GDPR)

- 3.1 The six Data Protection Principles, which the Association must adhere to when processing personal information, are set out as follows. Personal information must be:-
- Processed **fairly, lawfully and in a transparent manner** in relation to the Data Subject.
 - Collected for **specified, explicit and legitimate purposes** and not further processed for other purposes incompatible with those purposes.
 - **Adequate, relevant and limited to what is necessary** in relation to the purposes for which data is processed.
 - **Accurate** and, where necessary, **kept up to date**.

- Kept in a form that **permits identification of Data Subjects for no longer than is necessary** for the purposes for which the personal data is processed.
- Processed in a way 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.

4.0 THE LEGAL BASIS FOR COLLECTING PERSONAL INFORMATION

4.1 We can only process your personal information if it satisfies one of following conditions:-

- **Consent**—You have consented to your personal information being processed.
- **Contractual**—It is necessary for us to process your information to perform a contract or to take steps to enter into a contract. An example of this is processing your information in order to enter into a tenancy agreement with you or if you are a contractor to enter into a contract for services.
- **Legal obligation**—It is necessary for us to process your information in order to comply with a legal obligation.
- **Vital interests**—It is necessary for us to process your information to protect your vital interests for example a medical emergency.
- **Public tasks**—It is necessary for us to process your information to perform a task carried out in the public interest or in the exercise of official authority.
- **Legitimate interests**—It is necessary for us to process your information to see how we are performing so that we can meet our mission statement and objectives. Or in the prevention of fraud and reporting possible criminal acts or threats to a competent authority.

4.2 The Association will process information via the following means:-

- Housing Application forms
- Needs and Risk Assessment forms
- Support Plan forms
- Risk Assessment forms
- Via use of our website (see separate Website Privacy Notice)
- Via use of our CCTV equipment (see separate CCTV Privacy Notice)
- Tenancy Audits
- Tenancy Agreements

- Pre contractual information to supply services
- Contracts
- Bank References and Searches
- Data Processing forms
- Consent Forms
- Job application forms
- References
- Curriculum Vitae (CVs)
- Disclosure and Barring Services forms
- Declaration of Interest forms
- Telephone Calls
- Meetings
- Email
- Via third parties

4.3 Please note the above list is not an exhaustive list. Where information is considered sensitive information we will always seek your consent.

5.0 USE OF PERSONAL INFORMATION

5.1 We will only process your personal information for the purposes of:-

- Providing, managing and developing affordable housing.
- Providing property management & property maintenance services.
- Providing and managing support services.

5.2 We may also process information from you for the following reasons:-

- To prioritise and assess housing applications and complete tenancy sign-ups.
- To manage your tenancy.
- To meet your needs in our service delivery.
- To prevent fraud and illegal sub-letting and to confirm eligibility for housing.
- To assist with personal security and prevention and detection of crime.

- When you engage with our additional guidance, advice and support services.
- Provision of information requested by us may form part of a 'contractual requirement'.
- To understand how we are performing.
- To fulfil our legal obligations.
- To fulfil our contractual obligations

5.3 For further details please see the Association's Privacy Notice, which can be found on our website at www.csha.org.uk or alternatively you can contact us on 0208 467 9146.

6.0 YOUR RIGHTS AS A DATA SUBJECT

6.1 A Data Subject is a living individual whose personal information is processed by the Association. In the case of the Association, possible Data Subjects include Tenants, relatives of Tenants where their personal details are held by the Association, the Association's staff and individuals employed by suppliers or third parties who provide outsourced services. In accordance with the GDPR if you are a Data Subject you have the following rights:-

6.2 **The right to be informed** - Through the provision of privacy notices, we will be open and transparent about how and why we use your personal information.

6.3 **The right of access** - You have a right to ask us what personal information we hold about you and to request a copy of your information. This is known as a 'Subject Access Request' (SAR). Subject Access Requests must be made in writing, we have a Subject Access form you can use for this purpose. Written requests must be accompanied by proof of your address and identify.

If you are seeking to obtain specific information about a particular matter or from a particular time period, it helps if you clarify the details of what you would like to receive in your written request. If someone is requesting information on your behalf they will need written confirmation from you to evidence your consent for us to release this and proof of identity (both yours and theirs).

We have one month within which to provide you with the information you have asked for. However, we will be able to extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, we will inform you within one month of the receipt of the request and explain why the extension is necessary.

6.4 **The right to rectification** - You can ask us to rectify your personal data if it is inaccurate or incomplete. Please help us to keep our records accurate by

keeping us informed if your details change. We will must respond within one month. This can be extended by two months where the request for rectification is complex.

- 6.5 **The right to erasure** - The right to erasure is also known as ‘the right to be forgotten’. In some circumstances, you can ask us to delete or remove personal information, where there is no compelling reason for its continued processing. This is not an absolute right, and we will need to consider the circumstances of any such request and balance this against our need to continue processing the information. Our response will also be guided by the provisions of our Annual Data Cleansing and Retention Process and the Data Protection Policy.
- 6.6 **The right to restrict processing** - In some circumstances you can ask us to restrict processing, for example:-
- If you disagree with the accuracy of personal information.
 - If we are processing your information on the grounds of legitimate interests (as detailed earlier), and whilst we consider whether our legitimate grounds override those of yours.
 - When processing is restricted, you are permitted to store the personal data, but not further process it.
 - If we no longer need the personal information but you require the information to establish, exercise or defend a legal claim.
- 6.7 **The right to data portability** - This allows you to obtain and reuse your personal information for your own purposes across different services. It allows you to move, copy or transfer personal information we hold about you across different services, you may be able to ask us to do this.
- 6.8 **The right to object** - You can tell us if you object to our processing of your personal information, based on legitimate interests or for the purpose of direct marketing, including profiling.
- 6.9 **Rights in relation to automated decision making and profiling** - You can ask us to review any decisions that are determined by automated means. You can also object to our use of your personal information for profiling.
- 6.10 For further information on exercising these rights and what these rights mean, Data Subjects should contact the Data Protection Officer at csinfo@cscha.org.uk, or on 0208 467 9146.

7.0 SUBJECT ACCESS REQUESTS

- 7.1 A copy of the information should be provided free of charge. However, the Association reserves the right to charge a ‘reasonable fee’ when a request is manifestly unfounded or excessive, particularly if it is repetitive.

- 7.2 The Association may also charge a reasonable fee to comply with requests for further copies of the same information. The fee will be based on the administrative cost of providing the information.
- 7.3 Information will be provided without delay and at the latest within one month of receipt of the request. Where requests are complex or numerous the Association may extend the period of compliance by a further two months. If this is the case, the Association will contact the individual within one month of the receipt of the request and explain why the extension is necessary. The Association will take reasonable steps to ensure that the person asking for information regarding the data held on them is the person that the data belongs to.

8.0 PROTECTING YOUR INFORMATION

- 8.1 We will apply appropriate technical and organisational measures to ensure your personal information is secure. For example, we have systems in place to ensure that access to personal information is restricted to authorised individuals on a strictly need-to-know basis.
- 8.2 When we need to share personal information with our contractors and third party suppliers, our relationships are governed by our contracts and codes of conduct with them; which include strict data sharing and confidentiality protocols.
- 8.3 To help us ensure confidentiality of your personal information we will ask you (or any of your representatives) security questions to confirm your identity when you call us and as may be necessary when we call you. We will not discuss your personal information with anyone other than you, unless you have given us prior written authorisation to do so or where we have received a clear verbal instruction from you (as a one-off circumstance).

9.0 SHARING INFORMATION

- 9.1 Sometimes we need to share personal information we hold about you with other organisations that we work with or who provide services on our behalf. When sharing information we will comply with all aspects of data protection law and adhere to any information sharing protocols and codes of practice.
- 9.2 Where the information is of a sensitive nature, for example about your health, we will obtain consent from you prior to sharing this information, unless we are required or permitted to share this by law.
- 9.3 Where 'sharing' is in our 'legitimate business interests', we may share your information without seeking your consent first. This may be with:-
- Our contractors to facilitate repairs, maintenance or improvement works.
 - Debt and money management advisors.

- Local authority teams such as social services, environmental health and benefit agencies.
- Utility companies (and their representatives) and Council Tax Departments to ensure billing details are correct.
- Third parties providing services on our behalf. For example a mailing company distributing our newsletter; a research company carrying out a customer satisfaction survey, or a debt collection agency pursuing former tenant arrears.
- Agencies committed to protecting public funds and/or preventing fraud in line with the National Fraud Initiative.
- Police and other relevant authorities (e.g. Department of Work and Pensions, Probation Service, HM Revenue and Customs, in relation to the prevention and detection of crime, the apprehension of offenders or the collection of tax or duty.
- Other statutory organisations e.g. social services and health authorities as necessary for exercising statutory functions.
- We may also share information when required by law for example where ordered by the Court or to protect an individual from immediate harm.

10.0 PROMOTING OUR SERVICES AND CONTACTING YOU

- 10.1 If you are a Tenant we will routinely use your contact details to send you information and communicate with you about your tenancy. We will also tell you about events in your area. If you have a preferred method of contact, you can make this known to us, but we will use all means of contact available should we need to contact you in the event of an emergency or to enforce the terms of your tenancy.
- 10.2 We would also like to keep you updated with information about other services of ours and other reputable companies we work with, which do not form part of our core landlord services; but which we think may be of interest to you. Especially where this will assist us in meeting our objectives. This would include information such as accessing training and employment, financial guidance, energy efficiency and digital support. It is a legitimate business interest for us to send you postal communications (from time to time) which may comprise information about all these areas of our work. You can object to receiving this type of content from us in the post. Before sending electronic communications of this nature, we will follow the law and guidance which requires us to seek your consent. You can change your mind at any time. Please just contact us for more information.

- 10.3 We will never sell your personal information to third party organisations for marketing purposes.

11.0 RETENTION PERIODS

- 11.1 We will only hold information during the period of our relationship and for a set period afterwards to allow us to meet our legal obligations, including resolving any follow up issues between us. The Annual Data Cleansing and Retention Process sets out how long we keep different types of information for. This is based on National Housing Federation guidance, legal requirements and best practice. Please contact us if you would like any more information.

12.0 DEALING WITH PERSONAL INFORMATION BREACHES

- 12.1 A Personal Data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
- 12.2 The GDPR introduces a duty on the Association to report certain types of personal information breaches to the Information Commissioner's Office (ICO). If the breach of personal information is deemed significant in terms of the potential detriment to the Data Subject, the volume of information affected and the sensitivity of the information. The Association must do this within 72 hours of becoming aware of the breach, where feasible.
- 12.3 If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we will also inform those Data Subjects without undue delay. For example if the Data Subject is likely to suffer some form of damage like identity theft or leaves them open to financial loss.
- 12.4 The Association will keep a record of any personal data breaches, regardless of whether or not we are required to report them to the ICO.
- 12.5 If any individual suspects that there has been a breach they must follow the following process.

13.0 PROCEDURE FOR RAISING A CONCERN

- 13.1 Concerns relating to breaches of data must be reported to the Chief Executive who will be responsible for progressing matters, including liaising with other officers if necessary.
- 13.2 If, due to the nature of the concern, the report cannot be made to the Chief Executive, it should be reported directly to the Chair of the Association. The earlier a concern is reported, the easier it is to take action.
- 13.3 Concerns should, ideally, be raised in writing and should include as much information as possible including the background and history of the concern, names, dates, places and the reason for the concern. If there is any documentary evidence to support the concern, details of this should be

included. If it is not possible for the concern to be provided in writing, it can be reported by telephone or in a meeting with the Chief Executive.

- 13.4 In order for an investigation to take place, it will be necessary to demonstrate that there are sufficient grounds for an investigation. Other external professionals may be engaged outside of the Association and may assist with raising the initial concern and their advice may be sought before a report is made.
- 13.5 The action taken by the Association will depend on the nature of the personal information breach. The matters raised may:-
- Be investigated internally.
 - Be referred to the Police.
 - Be referred to the Information Commissioners Office.
 - Be investigated externally i.e. by the External Auditor.
- 13.6 In order to protect the Data Subject who is affected by the breach and or the Association, an initial decision will be made as to whether or not an investigation is appropriate and, if so, what form the investigation should take.
- 13.7 In some instances concerns may be resolved by agreed action without the need for an investigation. However, as mentioned earlier, if the breach of personal information is deemed significant in terms of the potential detriment to the Data Subject, the volume of information affected and the sensitivity of the information. The Association must report the breach to the Information Commissioner's Office within 72 hours of becoming aware of the breach, where feasible.
- 13.8 On receipt of a concern, the Association will write to the individual who raised the concern within 48 hours. The written response will include:-
- Acknowledgment of receipt of the concern.
 - An indication of how the matter will be dealt with.
 - The name of the person(s) who will deal with the response.
 - An estimate of how long it will take to provide a response.
 - An indication that further information will be required, if appropriate.
- 13.10 The Association will aim to conclude any investigation and report on the outcome within 10 working days, from when the concern was first reported.

This will include reporting back to the Data Subject and the individual who raised the concern.

- 13.11 This process is intended to provide a clear route for concerns to be raised within the Association and for the concerns to be dealt with and settled appropriately. However, if the individual who raises the concern or the Data Subject feels that this has not happened, they can contact the:-

The Data Protection Officer
Chislehurst and Sidcup Housing Association
45 Invicta Close
Chislehurst
Kent
BR7 6SJ
csinfo@csha.org.uk
0208 467 9146

or

Information Commissioner's Office
Wycliffe House, Water Lane
Wilmslow
Cheshire
SK9 5AF
Phone: 0303 123 1113
Email: casework@ico.org.uk
Website: www.ico.org.uk

14.0 MONITORING COMPLIANCE WITH THE GDPR

- 14.1 The Association will include data protection as part of its internal audit process to monitor compliance.
- 14.2 Every three years, there will be a formal review of data protection within the Association to ensure:-
- Policies and Procedures are up to date and comply with the law and best practice
 - Training and Awareness of data protection is embedded within the Association
 - The process for managing potential data breaches is fit for purpose
 - Privacy notices are up to date and comply with the law and best practice
 - Any associated documents continue to comply with the latest set of regulation advice or guidance
- 14.3 The Association also ensures risks associated with data protection form part of the risk management process of the Association and are reviewed on a regular basis.

15.0 TRAINING AND AWARENESS

15.1 All staff and Board Members must undergo training on data protection
In addition there will be:-

- Specialist training for Data Controllers, and Senior Management.
- Staff training and awareness of policies and procedures.
- Staff updates.
- Board training and awareness.

16.0 EXERCISING YOUR RIGHTS AND ANY QUERIES

16.1 For further information you can contact the Data Protection Officer at
Chislehurst and Sidcup Housing Association as follows:-

The Data Protection Officer
Chislehurst and Sidcup Housing Association
45 Invicta Close
Chislehurst
Kent
BR7 6SJ
csinfo@csha.org.uk
0208 467 9146

16.2 If you want to raise a complaint about the way we have processed your
information or would like to seek an independent view, or for independent
advice about data protection, privacy, e-privacy and data sharing issues, you
can contact the Information Commissioner's Office at the :-

Information Commissioner's Office
Wycliffe House, Water Lane
Wilmslow
Cheshire
SK9 5AF
Phone: 0303 123 1113
Email: casework@ico.org.uk
Website: www.ico.org.uk

17.0 REVIEW OF THIS POLICY

17.1 The Chief Executive is responsible for monitoring all concerns raised under
this policy and for reporting any concerns to the Board. The policy will be
reviewed by the Association every three years and/or in relation to any
regulatory, legislative guidance or best practice.