

Privacy Policy

Policy Owner:	Chief Technology Officer
Policy No:	CHI-POL-168
Version No:	002
Approval by:	• EMT • ARC
Date of Approval:	September 2023
Next Review Date:	September 2028

Version	Date of Changes	Changes made
001	01/09/2023	New Policy
002	05/08/2025	Moved onto new policy template Introduced document number and version control

Table of Contents

1. Policy Objective	3
2. Legislative & Regulatory Requirements	3
3. Scope & Definitions.....	3
4. Roles & Responsibilities	4
5. Personal Data Processed by the Group	5
6. Informing the Group's Data Subjects about Privacy	7
7. Data Subjects Privacy Notices	8
8. Website, Cookies & IP Addresses	9
9. Data Subjects Right to Complain	10
10. Adoption & Compliance Monitoring	11
11. Related Documents.....	11

1. Policy Objective

Chime Housing (“Chime”) and its subsidiaries (together “the Group”) is committed to protecting the privacy of, and information security relating to their Data Subjects. This Policy outlines the Group’s approach, as a Data Controller, to protecting all personal data that is collected, processed, held and shared about the Group’s Data Subjects and how the Group communicates this to them.

Chime takes customers’ privacy seriously and is committed to protecting their information through a range of measures and implements sufficient organisational and technical control measures to protect and safeguard all personal information under our control. The Group keeps up-to-date records of processing activities, decisions taken about processing activities and privacy risk assessments.

2. Legislative & Regulatory Requirements

Legislative

- General Data Protection Regulation (UK GDPR) & Data Protection Act 2018 (together “Data Protection Law”)
- Privacy and Electronic Communications Regulations (2003)

Regulatory

Regulator of Social Housing Governance and Viability Standard (para 1.1): “Registered providers shall ensure effective governance arrangements that..... comply with all relevant law.”

3. Scope & Definitions

Scope

This Policy covers all personal information that the Group processes about our various Data Subjects (as defined at section 3.2.3 below). It applies to all staff members including temporary and voluntary staff and Board/Committee members. Any breach of this Policy will be dealt with under the Group’s Conduct Policy.

Definitions

Data Asset Register (DAR): a “live” access-restricted log recording all processing activities taking place under the Group’s operating procedures which relate to our Data Subjects’ personal data. The DAR records all changes made to its content by date and author for audit trail purposes. It is available via the Data Champions, Deputy Chief Executive, Data Protection Officer and members of the IT support staff.

Data Controller: a company, organisation or individual who can decide why and how they will process personal data; they will decide whether to collect the data in the first place, what to collect, whom to share it with and how long to keep it for.

Data Subject: the person the Personal Data is about. As a Group, we have relationships with various Data Subjects including our tenants, leaseholders, shared owners, private market renters, staff, Board and Committee members, Gateway Membership Team, contractors and suppliers.

Chime's Group Data Protection Officer (DPO): an independent data protection expert who advises on and monitors a Data Controller's internal compliance with UK Data Protection Law and advises them about their obligations under it including through policy review and staff training/awareness. They may act as the central point of contact for enquiries from the controller's Data Subjects and may be contacted using the following email address: dpo@wcht.org.uk.

Personal Data: information about a living person who can be identified from either the information itself or additional information the Group may have or receive which is held electronically or in a structured filing system. Examples include names, contact information including emails and usernames, photographs and vehicle registration plates.

Chime Data Champion: a Chime staff member who acts as a central point of contact for their team/department in dealing with data protection queries and who takes an active role in ensuring data protection compliance for their team/department's work.

4. Roles & Responsibilities

Chime Group Board: is responsible for the Group's overall compliance with Data Protection Law, the operational responsibility for which is delegated to the Audit & Risk Committee (ARC) and Executive Management Team (EMT).

ARC: is the Group's collective data protection Board champion, responsible for monitoring the Group's overall compliance with Data Protection Law and relevant data protection policies. As such it will approve key data protection policies for the Group and receive regular reports on compliance from the Deputy Chief Executive.

EMT: is responsible for the Group's operational compliance with Data Protection Law and shall approve the main Group data protection policies.

Chime Group Staff, Board & Board Committee Members: are responsible for following and upholding this Policy in their day-to-day work for the Group, including in terms of responding to a request made by any of the Group's Data Subjects, to provide the relevant Privacy Policy or accompanying privacy information (see section 6.5 for further detail).

Deputy Chief Executive: is responsible for regularly updating ARC as to the Group's data protection compliance including any actual or potential breaches of Data Protection Law under this Policy or otherwise.

Chime's Group Data Protection Officer (DPO): is responsible for ensuring that this Policy and Procedure are upheld by the Group and enforced through appropriate staff training. The DPO will regularly review the Group's privacy content and data protection notices (as summarised at section 7 below) to ensure these are meeting the principle of transparency under UK GDPR and respect our customer's privacy. Where we fail this, the DPO will make recommendations accordingly.

Chime Data Champions: are responsible for maintaining an up-to-date Data Asset Register (see 5.1 below) so that:

- Any new data asset collected, processed or shared with a third party is recorded appropriately on the Data Asset Register; and that
- Any new point at which personal information is obtained from/about the Group's Data Subjects is recorded appropriately on the Data Capture Register tab of the Data Asset Register (see 6.3 below).

This will ensure that the Group continues to provide full and accurate privacy information to Data Subjects at the correct points of data capture.

5. Personal Data Processed by the Group

Chime maintains a Data Asset Register recording how the Group collects, stores and processes Personal Data belonging to its Data Subjects for various purposes. Further information is set out in the Data Asset Register Policy & Procedure but in the main these purposes are as follows:

Tenants

- Tenancy records to manage and support our various tenancies including where additional support is provided
- Rent & service charge account information
- Repair, maintenance and property adaptation records
- Customer feedback and satisfaction
- Records of tenancy changes (e.g. mutual exchange, succession or an application to purchase)
- Information about specific issues affecting the Group's customers / their household members (e.g. anti-social behaviour, safeguarding concerns, hoarding)
- Information about actual / suspected fraud
- CCTV footage
- Information about our membership

Leaseholders

- Information about the sale/purchase/assignment of a lease or its extension or about the sale of a freehold
- Information relevant to a lessee's mortgage application
- Information relevant to service/repairs/other charges
- Rent review information
- Information in connection with managing your business lease/tenancy

Staff

- recruitment & administration records (e.g. performance / absence management and employee relations matters).
- contractual and other benefits (such as pension) information.
- payroll records and bank account information.
- family/next of kin information.
- nationality/immigration information and criminal background.
- driving licence / qualifications & insurance information; and
- information about personal characteristics (e.g. ethnic origin).

Contractors, Suppliers & Other Third Parties

- Basic contact details and any other information they may share e.g. under a tender / bid process or otherwise in routine correspondence with us.

General enquiries and other information received

We will collect and process information voluntarily provided to us in the normal course of our business from other parties in accordance with our legitimate business interests. This will include contact and appointments with our members of staff.

CCTV

The Group may collect and store CCTV recordings in and around its properties where there is a clear legal ground to do so, including for the prevention and detection of criminal activity. For further information, see the CCTV Policy & Procedure.

The Group will process, store, retain and share personal information, where it is relevant and appropriate to do so for the purposes of responding to relationships with our customers, managing any general enquiries or other information received, volunteered or sent to us by the data subject that is or may be connected to any of our activities.

Information received under section 5 will be processed, stored, retained and shared in accordance with customers' rights, the Group's obligations under Data Protection Law, the general principles

contained within this Policy, the Group's Data Protection Statements and Privacy Notices, and the Group's Retention Policy.

We will search across our normal systems and servers in response to a wide-ranging request for personal data held about an individual under a DSAR, unless the person making the DSAR advises us otherwise or asks for specific personal information.

6. Informing the Group's Data Subjects about Privacy

Under Data Protection Law, we are required to give our Data Subjects certain information in order to make the processing of Personal Data relating to them fair and lawful.

This information should be provided at the point the Data Subject's Personal Data is first obtained by the Group. This is known as the 'data capture point'.

This information should also be provided whenever your processing purpose changes, if the data is transferred outside of the UK and/or the EEA, or if you share the data with any third parties. For example, if the data is shared, the provided information should list who (which parties) may have access to what data types, for what purposes, and under what legal bases.

We provide this information under a 'layered approach' to ensure that we provide the information at more than one opportunity. The Group therefore provides this privacy information through the following documents:

- a Data Protection Statement confirming who Chime Group is (i.e. as Data Controller in the relationship), (briefly explaining) why they are collecting the Personal Data they are collecting and referring the Data Subject to the more detailed Privacy Notice applicable to them for more information; and
- a Privacy Notice (previously called a 'fair processing notice') relevant to that Data Subject which, as stated above, explains more about how the Group process their Personal Data and manage their rights under Data Protection Law. It will detail to what standards, how, and when, the data will be stored and destroyed. It will also expand on the purposes of processing (such as legal bases); this is particularly important if the processing contains automated decision-making, as the Notice should identify the purpose, input data, and consequences of the automated processing. The Group's core Privacy Notice is their comprehensive 'Your Privacy Matters' booklet provided to customers.

The Group's Data Protection Officer maintains a record of all Data Protection Statements and Privacy Notices in the form of a Data Capture Register which forms part of the wider Chime Data Asset Register.

In line with the requirements of GDPR, the Group has issued new Privacy Notices to its various Data Subjects at specific points of their contact with us to ensure we have made our privacy policy readily available to them.

Dealing with Requests for Chime Privacy Policy/Information

If, however a member of staff receives a request from one of the Group's Data Subjects for privacy information relevant to them, they should refer to the Table at section 7.1 below to confirm the information which should be provided to them. Columns A and B confirm the type of Privacy Notice to be provided to each Data Subject. In the case of any query the DPO should be consulted.

Dealing with Data Subjects' Other Requests

If any of the Group's Data Subjects makes a request for a copy of their personal data or for it to be erased, transferred to another organisation, to stop being processed or corrected in some way, the request must be handled under the Subject Access Request or Information Rights Request Policies & Procedures.

7. Data Subjects Privacy Notices

The Privacy Notices to be provided to Data Subjects at each are set out below together with the Data Capture Points at which the Privacy Notice is first supplied to the Data Subject.

(A) Data Subject	(B) Privacy Notice	(C) Data Capture Point
Tenants	'Your Privacy Matters' Booklet	Tenant sign-up (all tenure types, mutual exchange, internal transfer, tenancy assignment and succession).
Members	'Your Privacy Matters' Booklet	Upon member election
Leaseholders	Leaseholder Privacy Booklet	S20 Consultation letter Successful Right to Buy/Acquire application
Tenant / Leaseholder user of Digital Tenancy Services	Chijme Privacy Policy	DTS Privacy Policy tab
Tenant / Household Member with 'Alert1', 'VULNBL' or 'Permission to Speak' UDC applied to relevant Orchard Tenancy ID	Letter sent under Person UDC Policy & Procedure	Application of relevant UDC
Visitor to Chime premises	Public notice re CCTV recording	Displayed at CCTV site

Caller to CSC	IVR message	Inbound telephone call
Chime job applicant	Recruitment Privacy Statement	Networkx account creation LinkedIn Jobs page
Employees, contractors, agency workers, Board & Board Committee members, volunteers & interns	Human Resources Privacy Booklet	Enclosure with formal offer letter
Stakeholders, suppliers, contractors & other 3 rd parties	Chime Privacy Policy	Link on all outgoing email signatures
Website visitor	Website Privacy Policy	Website homepage view

8. Website, Cookies & IP Addresses

Chime also captures certain information from its website (www.wcht.org.uk) through the use of cookies and other technology. These are used to help us understand and improve customers' experience when using our website. This section explains how we use our website, what our cookies are and how we use them.

When customers access our website, they will receive a notification informing them that our website uses cookies along with an option of whether to browse using cookies along with a link to our Privacy Policy. Customers can choose not to use cookies by not accepting the option and still access our website without enabling the cookies. Further information about cookies see 8.6 below or visit <http://www.allaboutcookies.org/>.

IP Addresses: An Internet Protocol (IP) address is a set of numbers which is automatically assigned to a visitor's computer whenever they log on to their internet service provider or through their organisation's computer network. Their computer is identified by the IP address assigned to it during their session on the Internet.

Chime and/or third-party companies acting on its behalf may collect IP addresses for the purposes of systems administration and to audit the use and activity of the website.

Chime do not link a visitor's IP address to any other personal information that may be held about them. Therefore, the visitor to the website remains anonymous.

Cookies: Chime's website uses a technology called 'cookies'. Cookies are small computer text files placed in the visitor's computer's memory by the computer which provides or 'hosts' the website. Cookies are not spyware or a computer virus but are used to make surfing the internet easier.

Session Cookies: Chime only use Session Cookies on its website for the purpose of maintaining the site, to improve functionality and delivery of the webpage on the device that you are viewing

the webpage from. They can also be used to track the total number of visits to the website for the purpose of improving the services that we offer.

Session cookies are temporary and are erased when you close your browser. They do not store any personal information about the visitor, their computer, visit or browsing history.

Google Analytics: Chime uses Google Analytics for our website, that also uses first party cookies, to improve the performance and user experience on our website and for our own marketing purposes to enhance the content on the site. These cookies use information in aggregate form and uses the minimum default rather than recommended settings. This is to ensure that the minimum amount of information is received by Google and an approach taken to maximise your privacy protection. Google stores cookie information on servers located in the United State and does not associate your IP address with any other data held by Google.

Cookie management: Visitors to the website have the ability to accept or decline cookies. By default, all cookies are disabled. By accepting the cookies, visitors consent to the processing of data about them by Chime and Google Analytics for the purposes set out above.

Visitors also have the ability to accept or decline cookies through their internet browser software and can modify these settings to accept, decline and remove cookies if they prefer.

Other privacy matters relating to the website: Personal information is captured through the website when visitors voluntarily submit information about themselves, for instance when they submit a CV or a request for further information. This information is only used for the specific purpose for which it is submitted for.

Chime's website may provide links to third party websites as a service to our users. The privacy statement described in this Policy does not apply to those sites. Users should ensure they check the legal and privacy statement posted on each site they may link to.

We may occasionally update the privacy statements set out within this Policy. We encourage visitors to periodically review the statement to stay informed about how we are helping to protect the information we collect. Visitors continued use of the website constitutes their agreement to the privacy statement and any updates thereto.

9. Data Subjects Right to Complain

If any of the Group's Data Subjects wish to complain about our handling of their Personal Data under this Policy and/or that their right to privacy has been compromised, they should contact the Group's Data Protection Officer (DPO) at dpo@wcht.org.uk.

If the Data Subject is not satisfied with the response, they receive from the Chime Group or on its behalf, they have the right to lodge a complaint with the supervisory authority. In the United Kingdom this is the:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
(t) 0303 123 1113

10. Adoption & Compliance Monitoring

Issued to all staff employed by the Group, Board members and Committee Members as a 'mandatory read' document prior to its implementation. It will then be reviewed annually or following any change to its content.

Staff awareness of and compliance with this Policy shall be measured by:

- i. Reporting to the relevant Director instances of non-compliance with the mandatory read circulation of this Policy; and
- ii. Monitoring all instances of staff responding incorrectly to a Data Subject's enquiry about the Group's' approach to privacy or request for a copy of their relevant Privacy Notice.

This Policy shall be monitored annually by the DPO by reviewing the number (if any) of complaints made by the Group's Data Subjects to either the DPO or the ICO of any breach or potential breach of this Privacy Policy. All and any breaches or near miss incidents will be reported by the Deputy Chief Executive to ARC in accordance with section 4 above.

11. Related Documents

- Information Governance and Information Security Framework of Policies
- CCTV Policy & Procedure