Customer Records Policy

Originator:	Policy and Strategy Team
Executive Management Team Approval Date:	21st June 2022
Review date:	June 2025

1	Introduction
1.1	One Vision Housing (OVH) aims to provide excellent customer relationship and tenancy management services on a consistent basis.
1.2	To achieve this aim OVH will make effective use of the information it gathers and maintains about customers and the interactions with them, to constantly improve service delivery, achieve efficiencies and ensure it meets individual needs.
1.3	The Customer Records Policy outlines the types of information that it is recorded about customers, how it is used and the systems that are in operation to ensure it is held securely.
1.4	The application of the Policy ensures compliance with the Regulatory Framework for Social Housing in England as adopted by the Regulator for Social Housing (RSH) as outlined below: • **Understanding and responding to the diverse needs of tenants** o Treat tenants and prospective tenants with fairness and respect o Understand the diverse needs of tenants, including those arising from protected characteristics, language barriers, and additional support needs • **Customer service, choice and complaints** o Ensure their approach to handling complaints is simple, accessible and publicised
1.5	**Scope of the Policy**
1.5.1	The Customer Records Policy covers all information that is held about existing OVH customers that access housing management services (for rent, shared ownership and outright sale) and with whom it has a contractual relationship.
1.5.2	The Policy covers information that is provided by and to customers in written form, is captured by electronic means and through direct communications either face-to-face or via telephone.

1.5.3	The Policy also covers customer information and records that are shared with internal and external partners in the legitimate delivery of OVH business activities, ensuring compliance with all relevant UK data protection legislation.
1.5.4	Potential customers whose details OVH may have access to e.g. on shared systems used for recording housing applications are outside of the scope of this Policy. OVH will, however, apply good information security practices to this data and it will be subject of confidentiality agreements.
1.6	Access and Communication
1.6.1	OVH is committed to ensuring that its services are accessible to everyone. OVH will seek alternative methods of access and service delivery where barriers, perceived or real may exist, that may make it difficult for people to work for OVH or use its services.
1.6.2	Working with our customers we have established a Vulnerable Persons and Reasonable Adjustments Policy to ensure we make best use of every customer interaction to meet customers' needs in our service delivery and ensure this information is kept up to date.
1.7	Equality, Diversity, Inclusion and Human Rights
1.7.1	OVH is committed to ensuring that no person or group of persons will be treated less favourably than another person or group of persons and will carry out our duty with positive regard for the following protected characteristics within the Equality Act 2010; Age, Disability, Gender, Race, Gender Identity / Gender Expression, Sexual Orientation and Religion and /or Belief, Pregnancy and Maternity, Marriage and Civil Partnership.
1.7.2	OVH also recognises that some people experience disadvantage due to their socio-economic circumstances, employment status, class, appearance, responsibility for dependants, unrelated criminal activities, being HIV positive or with AIDS, or any other matter which causes a person to be treated with injustice.
1.7.3	OVH will also ensure that all services and actions are delivered within the context of current Human Rights legislation. OVH will endeavour to ensure its staff and others with whom it works, will adhere to the central principles of the Human Rights Act (1998).
1.8	The Policy should be read in conjunction with: • OVH Information Management Policy • OVH Data Protection Policy
2	**Statement of Intent**
2.1	When collecting, processing, storing and disposing of customer information, OVH will ensure that it complies with all relevant UK data protection legislation.
2.2	OVH will ensure that accurate records are maintained of all significant interactions and communication it has with its customers, however this occurs, including but not limited to face-to-face conversations, telephone calls, web chat, letters, email, SMS, web contact forms, social media etc.

2.3	The information recorded will not always be a verbatim 'word for word' of the contact unless it is necessary to facilitate the service request or is otherwise significant e.g. in meeting individual needs, is in connection with appeals and complaints or is in relation to any legal matter.
2.4	In maintaining customer records OVH aims to ensure: • It meets individual customer communication and support needs • It provides streamlined services with effective communication and co-operation between teams and partner agencies via one point of contact • Records are kept up-to-date and can be revised easily at the customer's request • It reduces the need for unnecessary contacts and leads to quicker problem resolution and better service delivery
2.5	In addition to information that is held about individual customers, OVH will analyse collective customer information and contacts, in anonymised form, to identify service improvement opportunities, to determine resource provision and ensure groups that share protected characteristics are not disadvantaged in any way.
2.6	When in the course of genuine business activities OVH shares customer information with organisations within and external to the Sovini Group, it will ensure that appropriate confidentiality agreements are in place and that they have secure means of data transfer and storage.
3	**Policy**
3.1	OVH will maintain a record of all verbal, written and electronic communications with its existing customers. This will not, however, include general communications or information items that are intended for all customers e.g. tenants' newsletters.
3.1.1	OVH has a number of secure electronic systems for capturing these contacts and communications including a general customer relationship management system, specialist systems for recording anti-social behavior (ASB) cases and interactions that occur in the Independent Living service.
3.1.2	OVH staff will access information within a file or system based on a series of permissions that are commensurate with the staff member's role and seniority. Information that is of a sensitive nature will be held on a need-to-know basis and viewing rights will be restricted to managers with specific responsibilities and those with system administrator rights.
3.1.3	Where customers clearly indicate that they want the nature and contents of their verbal and written communications with OVH to remain anonymous and not be recorded against their personal records, OVH will comply with these wishes. Examples of where this may occur is when customers wish to report ASB cases or safeguarding alerts but do not want their identity to be known.
3.1.4	In these circumstances OVH will record the concern or alert being made and will take appropriate action or make the appropriate referral. This will not, however, be recorded against the personal record of those raising the concern.

3.1.5	The only circumstances when OVH would consider overriding the request for anonymity is when there is a court order, police request or a person's 'vital interests' are concerned, where recording and sharing information is critical to prevent harm, distress or is required for medical or safeguarding intervention measures.
3.1.6	In meeting best interests, OVH will be mindful of the requirements of the Mental Capacity Act 2005 and will assume customers have full capacity to make reasonable decisions, at a time when they need to be made.
3.1.7	Where there is a reasonable belief that a person 'lacks capacity' to make a decision at a time when it needs to be taken and where it is in their 'best interests', OVH may request a formal assessment of capacity be carried out by a relevant and qualified health practitioner and may do so without their consent.
3.1.8	Where an assessment has taken place and it is found that a person lacks sufficient capacity, OVH may share personal information, where it is in the best interests on a need-to-know basis, with • Anyone previously named by the person as someone to be consulted on either the decision in question or on similar issues • Anyone engaged in caring for the person • Close relatives, friends or others who take an interest in the person's welfare • Any attorney appointed under a Lasting Power of Attorney or Enduring Power of Attorney made by the person • Any deputy appointed by the Court of Protection to make decisions for the person • External agencies as required e.g. police, social care, mental health and health care services
3.1.9	If an assessment by a relevant and qualified health practitioner takes place and the customer is deemed to have sufficient capacity and they have previously requested information they provide is not held against their personal records, this will subsequently be removed and safely disposed of, and section 3.1.8 will apply.
3.2	Verbal Contacts
3.2.1	OVH will endeavor to keep a record of all verbal communications and interactions it has with customers including but not exclusive of the following: • Inbound telephone conversations • Outbound telephone conversations • Attempted outbound telephone contact where the customer does not answer (including whether a voicemail message is left or not) • Customers calling into any OVH offices • Pre-arranged appointments at OVH offices or any other location, including no access cases or failure to attend appointments • Contact made as a result of Officers 'door-knocking' • Contact made with customers during Neighbourhood walkabouts where a request for service is made by the customer

3.2.2	As indicated in 2.3 above, the record will not always be an exact recording but will contain sufficient, summarised detail e.g. the method of contact, the time and date of the contact, the subject matters discussed and any further actions that will result.
3.3	Written and Electronic Communications
3.3.1	OVH will keep a record of all written communications that are sent to, or received from, customers against their personal electronic files in line with the Data Retention Schedule. This will include system generated letters such as those that are sent in connection with rent account management.
3.3.2	This will also apply to all communications that are sent or received via email or web contact forms.
3.3.3	Where communication is sent or received via social media, a record will only be kept against a customer's personal records when it involves a request for service and a response is required.
3.3.4	When scanning documents for electronic storage, OVH will ensure they are indexed against the correct system for the matters they are concerned with. OVH will also ensure the integrity of sensitive and confidential information is maintained at all times.
3.3.5	This includes having appropriate confidentiality measures in place with any third party who may process customer information and records of interactions on OVH's behalf.
3.3.6	Where possible OVH will disaggregate general requests for service from sensitive information when this is received together and by OVH staff entering vital details on the correct system e.g. requests for repairs will be stored and processed separately from reports of ASB.
3.3.7	It may, however, not always be possible to achieve a neat split of information received in written format and in these circumstances OVH will rely on the professionalism of its staff to achieve a 'best fit' for indexing purposes. This will include when information is transferred between systems or is used to prompt workflows.
3.3.8	OVH will also advise customers that have submitted written information or requests that contains both general service requests and confidential information that it would aid accurate and secure record keeping, if this is submitted separately going forward.
3.4	Customer Call Recording
3.4.1	In line with the provisions set out in the Privacy Notice (available at https://ovh.org.uk) the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 ('LBP Regulations'), the Regulation of Investigatory Powers Act (RIPA) 2000 and any relevant telecoms class licences, OVH may record inbound and outbound calls with customers for the purposes of: • Training and quality management • Fact verification • Evidence of a business transaction • Any other legitimate public task in the discharge of its business operations e.g. evidence gathering for breaches of a tenancy agreement such as anti-social behaviour

3.4.2	Customers contacting OVH may also choose to record telephone conversations as long as they request consent to do so, this consent is confirmed by the OVH staff member, and the recording is for personal use only i.e. not shared in any way with third parties.
3.4.3	If customers have a legitimate reason for wanting to record a telephone conversation with OVH e.g. they have a condition which impacts on memory, they should advise the OVH staff member at the start of the telephone conversation and before starting any recording device.
3.4.4	If an OVH staff member has good reason to believe that a telephone conversation is being recorded and they have not been advised by the caller, and / or they have not consented to the recording, then they are able to challenge the caller.
3.4.5	The member of staff can advise the caller that they do not give their consent for the call to be recorded and may terminate the call. The call can be terminated, once the intention to do so, has been made clear to the caller.
3.4.6	In these circumstances the staff member should also advise the customer of other methods of communication e.g. via letter or email.
3.4.7	The member of staff must add notes to the relevant records on the CRM system explaining the events once the call has been terminated. In all instances, the staff member's Team Leader or Line Manager should be informed.
3.5	Use of Customer Profile Information
3.5.1	OVH requests all customers (as defined in 1.6.1) to provide 'profile' information at the point they access OVH services e.g. make applications for housing or signing-up for properties. In addition to core data e.g. name, age, etc. which must be provided, OVH will request information on a customer's personal characteristics e.g. any disabilities or if English is not spoken as a first language, on a voluntary basis.
3.5.2	This additional profile information is used to create a general profile of people who use OVH services and to identify any potential barriers that may prevent any group from accessing services.
3.5.3	The profiling information that relates to the individual characteristics would only be used to alter the method of service delivery and support provided with the express permission and consent of the individual (in line with UK data protection and GDPR requirements).
3.5.4	Examples of how OVH will alter service provision include sending written communications in a preferred format, allowing additional time for answering calls and visits for those with mobility problems and showing respect for religious customs.
3.6	OVH Information Security
3.6.1	To meet all legal requirements and to ensure customer information OVH holds, is protected from unauthorised access, modification, disclosure, destruction and is only used for the purposes in which it is intended, it operates a number of safeguarding measures, including: • Secure Information Technology systems which are accredited to the following standards:

	○ ISO 27001 Information Security Management Systems ○ ISO 27701 Privacy Management Systems certifications ○ Cyber Essentials • All staff agree to abide by OVH Computer User Code of Operations, use strong and complex passwords and have signed Confidentiality Agreements when using OVH systems and when processing customer information • Confidentiality agreements and means of secure transfer when customer information is shared with third parties, for legitimate business purposes • Operation of robust Data Protection and Information Management Policies
4	**Implementation**
4.1	All OVH staff have a responsibility for maintaining the integrity of customer information and records and will receive training on the correct use of OVH systems.
5	**Performance**
5.1	There are no specific performance targets as a result of the operation of this Policy.
5.2	As part of overall data protection conformance, OVH aims to have zero reportable breaches to the Information Commissioners Office. Should any reportable breaches occur OVH would report by exception to the Risk and Audit Committee, including any remedial actions required.
6	**Consultation**
6.1	All OVH staff have been consulted in the development of this Policy. The Tenant Policy Review Group were also consulted on the development of this Policy on 08/04/2022.
7	**Review**
7.1	The Customer Records Policy will be reviewed every two years, as near as is possible from the date of Executive Management Team (EMT) approval or as required by the introduction of new legislation, regulation or as a result of OVH system audits. The review process will ensure its continuing suitability, adequacy and effectiveness.
8	**Equality Impact Assessment**
8.1	Was a full Equality Impact Assessment (EIA) required?	Yes
8.2	When was EIA conducted and by who?	An Equality Impact Assessment undertaken by the Policy and Strategy Manager and the Policy Writer on 24-03-22

8.3	**Results of EIA**	No adverse or differential impacts for any group with protected characteristics were identified as a result of the operation of the Policy.
9	**Scheme of Delegation**	
9.1	**Responsible committee for approving and monitoring implementation of the Policy and any amendments to it**	EMT
9.2	**Responsible officer for formulating Policy and reporting to committee on its effective implementation**	Director- Compliance and Governance
9.3	**Responsible officer for formulating, reviewing and monitoring implementation of procedures**	Director- Compliance and Governance

10	**Amendment Log**		
Date of revision:	**Reason for revision:**	**Consultation record:**	**Record of amendments:**
1st May 2018	In line with review schedule	See section 6	The Policy has been rewritten throughout and ensures compliance with revised data protection legislation
02 June 2020	In line with review schedule	See section 6	• Change at 3.3.1 – inclusion that OVH will keep a record of all written communications that it gets in line with the Data Retention Schedule • Change at 3.5.1 – Inclusion of standards which the OVH's Secure Information Technology systems is accredited to
21st June 2022	In line with changes in business practice	See section 6	• Change at 3.4- inclusion of a section 'Customer Call Recording' • Change at 1.1- Inclusion of