OVH Data Protection Policy

Originator:	Policy and Strategy Team
Executive Management Team Approval Date:	September 2021
Review date:	September 2024

1	Introduction
1.1	One Vision Housing (OVH) collects and uses Personal Data about people with whom it deals with in order to operate as a business. This data covers current, past and prospective employees, suppliers, customers, board members, contractors and others with whom it communicates.
1.2	This Policy sets out OVH's responsibilities for dealing with all personal information, however it is collected, recorded and used. It relates to all information for which OVH is the Data Controller (defined as the organisation and not the employees).
1.3	The Policy meets the following OVH corporate aims: • To provide the environment to deliver business success • To provide homes that meet demand, in safe, secure and sustainable neighbourhoods • To provide excellent services that meet or exceed customer and stakeholder expectations • To make a positive impact in the communities in which we operate
1.4	The Policy ensures OVH complies with all applicable data protection legislation, including the provisions set out in the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. OVH will also ensure it is prepared for any changes to be introduced under the Data (Use and Access) Bill when this is approved as UK legislation.
1.5	The application of this Policy ensures that OVH complies with the outcomes of the Regulatory Framework for Social Housing in England as follows: • Ensure that communication with and information for tenants is clear, accessible, relevant, timely and appropriate to the diverse needs of tenants • Registered providers shall ensure effective governance arrangements that deliver their aims, objectives and intended outcomes for tenants and potential tenants in an effective, transparent and accountable manner. Governance arrangements shall ensure registered providers: o Adhere to all relevant law

- Comply with their governing documents and all regulatory requirements
- Are accountable to tenants, the regulator and relevant stakeholders
- Safeguard taxpayers' interests and the reputation of the sector
- Have an effective risk management and internal controls assurance framework
- Protect social housing assets

1.6 Access and Communication

1.6.1 OVH is committed to ensuring that our services are accessible to everyone. We 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 us or use our 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 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 core strands of equality; Age, Disability, Gender, Race, Gender Identity/ Expression, Sexual Orientation, Marriage and Civil Partnership, Pregnancy and Maternity, Religion and/or Belief.

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. Staff and others with whom we work, will adhere to the central principles of the Human Rights Act (1998).

1.8 This Policy should be read in conjunction with:

- OVH Information Management Policy
- OVH CCTV Policy
- OVH Customer Records Policy
- OVH Maintaining Professional Boundaries Policy
- OVH Privacy Policy

2 Statement of Intent

2.1 In operating this Policy, OVH will comply with the principles outlined in the relevant Data Protection Legislation, which requires that personal information is:

	(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency'); (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation'); (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'); (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy'); (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the Personal Data are processed; Personal Data may be stored for longer periods insofar as the Personal Data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation'); and (f) 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 ('integrity and confidentiality')
2.2	OVH have a designated Data Protection Officer (Data and Quality Assurance Manager) who takes a lead role for responding to data protection enquiries and for ensuring systems for data capture, storage and disposal are fit for purpose.
2.3	OVH will respond to all requests for data protection information promptly and courteously. OVH will acknowledge all requests for data protection information, submitted either verbally or in writing, within three working days and, subject to verification of identity being confirmed, will provide a full response within 1 month (the corresponding date in the following month from receipt of the request), including requests for images captured by OVH owned CCTV systems.
2.4	OVH will provide all new staff with data protection and information security training as part of their induction process and all other staff will receive refresher training as required on request. All staff will be required to comply with the OVH Computer Users Code of Operation and be made aware of their responsibilities for data protection via the OVH Staff Handbook.
2.5	OVH will adhere to the latest guidance notes and codes of practice produced by the Information Commissioner's Office, and these will be made widely available to OVH staff via internal document control systems. OVH is registered with ICO as its Data Protection regulatory authority.

2.6	OVH will comply with any recommendations or judgements made by the Information Commissioner's Office should it be found to be in breach of any relevant Data Protection Legislation.
3	**Policy**
3.1	Data Protection Definitions
3.1.1	For the purposes of this Policy and in compliance with relevant Data Protection Legislation the following definitions will apply: • OVH as an organisation (and not its employees) will be the Data Controller - who decide how `Personal Data' is `Processed' and for what purposes • 'Processing' of data or information (not just Personal Data) includes obtaining, recording, holding, organising, adapting, consulting, retrieving or otherwise performing some operation on it including disclosure of data. OVH remains the Data Controller even when the processing may be carried out by a third party that OVH shares the data with, for legitimate business purposes • 'Personal Data' is all data relating to a living individual who can be identified either from that data or from other information in the possession of the Data Controller. It includes expressions of opinion about that individual as well as any intentions that any person has regarding that individual. It also includes information likely to come into the Data Controllers possession (OVH) as well as data in OVH's possession • Personal Data also includes a specific sub-category known as Special Categories of Personal Data 'Sensitive Personal Data'. This includes Personal Data which the Data Protection Legislation deems is sufficiently sensitive to warrant its own handling requirements owing to the potential damage that could result if it is not handled correctly. Sensitive Personal Data includes: o race; o ethnic origin; o political opinions; o religious or philosophical beliefs; o trade union membership; o genetic data; o biometric data (where this is used for identification purposes); o health data; o sex life; or o sexual orientation • Although not in the list above, Data Protection Legislation states that information relating to criminal convictions or offences should also be handled with an increased level of care owing to its sensitivity • A Data Subject – is the person about which Personal Data is held
3.2	Data Protection Usage
3.2.1	OVH will only collect, store and use Personal Data for legitimate business purposes and will not forward on the information held to any third parties that may cause personal detriment or where such sharing of Personal Data has not been identified to the Data Subject in accordance with OVH's relevant Privacy Policy.

3.2.2	Where a law enforcement agency seeks Personal Data to assist in the apprehension of an alleged offender, the `crime exemption' may apply. Any such requests for disclosure should be forward to the Data Protection Officer.
3.2.3	Any Sensitive Personal Data OVH holds about a person will only be used for statistical purposes, to tailor services to meet individuals' needs or to ensure the organisation fulfils its aims outlined in the OVH Equality, Diversity and Inclusion Policy.
3.2.4	Occasionally it will be necessary for OVH to share Personal Data it holds about individuals for legitimate business purposes and to provide housing related services. An example here is the sharing of names and addresses of customers with those who OVH employs to provide maintenance and repair services.
3.2.5	Where these companies are within the Sovini Group they will be subject to Group wide confidentiality statements and protocols surrounding the use of shared computer systems that are designed to protect the integrity and misuse of Personal Data.
3.2.6	Where OVH is required to share Personal Data with third parties outside of the Sovini Group on a regular basis it will endeavour to ensure legal agreements are in place between the two organisations.
3.2.7	This can take the form of a contract, a confidentiality agreement or data processing agreement and will set out standards that the organisations will adhere to in processing of Personal Data, namely: • That they will only use the Personal Data for the purposes for which it was intended • They will keep the information secure and prevent unauthorised access • That they will meet the requirements of the relevant Data Protection Legislation and will assist OVH in meeting these requirements
3.2.8	In addition to the above agreements, OVH will publish on its website a Privacy Policy which in broad outline will state: • The legal basis why we process personal information • The systems and practices we deploy to keep the information secure • What purpose we are processing it for • Whether you have to provide it to us • Whether there are other recipients of your personal information and examples of the types of organisations that we may need to share your information with • Your rights as Data Subject
3.2.9	Where it is necessary to request or share Sensitive Personal Data with third parties, OVH will endeavour to obtain specific consent from the individuals concerned. However, in certain instances where it is a legal requirement OVH is permitted to share Personal Sensitive Data and in such cases, consent is not required. Where applicable, the consent agreement will broadly outline: • The name of your organisation with whom OVH is sharing or requesting the information; • The name of any third-party controllers who will rely on the consent; • Why we want the data;

- What we will do with it; and
- That individuals can withdraw consent at any time

3.3 Data Storage

3.3.1 OVH will maintain high standards of data security at all times and will ensure:

- All employees are aware of and abide by the OVH Computer User's Code of Operation
- There are appropriate measures in place to protect Personal Data including password protected computer systems, confidential waste arrangements, secure office accommodation and good practice guidance issued to staff on storage of paper based Personal Data
- Sensitive Personal Data e.g. Police restricted information or adult / children social care data is held outside of Customer Records Management systems and access is controlled to authorised staff only
- Contracts exist with any third-party data processor who processes information on OVH's behalf

3.4 Data Disposal

3.4.1 OVH will only hold and store Personal Data for as long as required within the provisions of the relevant Data Protection Legislation. When disposing of Personal Data, OVH will only use registered confidential waste carriers that can provide certificates of destruction.

3.4.2 OVH will also comply with the Waste Electrical and Electronic Equipment Directive (WEEE) when disposing of computer equipment and will ensure computer hard drives are effectively cleansed to prevent any loss of Personal Data.

3.5 Access and the rights of the data subject

3.5.1 In compliance with the relevant Data Protection Legislation, OVH will ensure that when individuals request, either verbally or in writing, access to personal information that OVH holds about them, they will:

- Be told whether Personal Data is being processed, and if so:
    - Be told what data is being processed, why and to whom that data may be disclosed
    - Be given a copy of the information or data in an intelligible form
    - Be told the source of the data

3.5.2 In addition, and specifically in compliance with Data Protection Legislation, Data Subjects will also have the rights to the following:

- The right to rectification (to have the Personal Data OVH hold about them to be changed or updated)
- The right to erasure (the right in certain circumstances for information to be safely disposed of)
- The right to restrict processing (the right where specific legal circumstances apply – as outlined in the UK GDPR, for processing to be changed or stopped, normally this would only be for a specific period of time)

- The right to data portability (for data to be transferred to another Data Controller or processor at the Data Subject's request)
- The right to object (to processing of information for specific purposes – refer to UK GDPR for details)

3.5.3 The Data Protection Officer will be the designated person within OVH for dealing with all data protection requests for information, including requests for the release of images captured by the OVH CCTV System.

3.5.4 In most circumstances OVH will comply with requests for access to personal information free of charge and would only consider charging a reasonable administrative fee, equivalent to the cost of retrieving the information, if the request is manifestly unfounded, excessive, or if repeat requests are made. Where a charge is to be levied, OVH will inform the Data Subject, and payment will need to be received before copies of data are released.

3.6 Exemptions

3.6.1 OVH will not normally share or pass on Personal Data to any third parties, without explicit consent (See 3.2.8 above for details). There are, however, a number of exemptions allowed within the Data Protection Legislation where OVH may consider sharing information, as outlined below:

- The sharing is for the assessment of any tax or duty
- The sharing is necessary to exercise a right or obligation conferred or imposed by law (other than an obligation imposed by contract)
- The sharing is for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings)
- The sharing is for the purpose of obtaining legal advice
- The sharing is for research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress)
- The Data Subjects have given their consent
- The sharing is for the prevention or detection of crime

3.6.2 In addition to the above, there may be other circumstances where OVH will share information with third parties when the public interest in sharing the information outweighs the public interest in protecting confidentiality. Examples include:

- Where safeguarding concerns exist
- Where a person's 'vital interests' is concerned i.e. where sharing information is critical to prevent harm, distress or is required for medical intervention measures

3.6.3 In sharing Personal Data OVH will always be mindful of the requirements of the Mental Capacity Act 2005 and will adhere to the statutory principles of:

- A person must be assumed to have capacity unless it is established that they lack capacity.
- A person is not to be treated as unable to make a decision unless all practicable steps to help him to do so have been taken without success

- A person is not to be treated as unable to make a decision merely because he makes an unwise decision
- An act done, or decision made, under this Act for or on behalf of a person who lacks capacity must be done, or made, in his best interests
- Before the act is done, or the decision is made, regard must be had to whether the purpose for which it is needed can be as effectively achieved in a way that is less restrictive of the person's rights and freedom of action

3.6.4 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.

3.6.5 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

3.7 Data Sharing Protocols

3.7.1 OVH will ensure data sharing protocols that exist with the Police and Local Authorities in the areas it operates adhere to guidance produced by the Association of Chief Police Officers and Association of Directors of Social Services. This will include personal information relating to individuals this is shared in public protection forums such as:

- Safeguarding Boards (adults and children)
- Multi-agency risk assessment conferences (MARACs)
- Multi-agency public protection arrangements (MAPPAs)

3.8 Use of CCTV Images

3.8.1 All CCTV images that are captured by OVH are subject to the relevant Data Protection Legislation. In line with national guidelines CCTV images will be stored for as long as necessary to meet the purpose of recording them (up to 30 days in line with national guidelines). The rights of the Data Subject to view CCTV footage are as outlined above in section 3.5. For further details see the OVH CCTV Policy.

3.9 Reporting a Personal Data Breach

3.9.1 The Data Protection Legislation requires Data Controllers, such as OVH to notify any breach of Personal Data to the ICO and, in certain instances, the Data Subject. A Personal Data Breach includes any act or omission that compromises the security, confidentiality, integrity or

	availability of Personal Data or the physical, technical, administrative or organisational safeguards that OVH or its third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.	
3.9.2	OVH has put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or the ICO where we are legally required to do so.	
4	**Implementation**	
4.1	The OVH Data Protection Policy applies to all staff and there is a collective responsibility to ensure adherence to the principles (outlined above in section 2.1).	
4.2	All staff have a responsibility to inform the Data Protection Officer via their line manager if they become aware of any breaches of data protection. Any staff member that knowingly breaches data protection that leads to personal detriment may be subject to relevant disciplinary procedures.	
4.3	It is the responsibility of the Group Director Governance and Compliance to ensure this Policy, and the supporting procedures are effectively implemented.	
5	**Performance**	
5.1	OVH aims to have 100% compliance with the requirements of the relevant Data Protection Legislation. OVH will record any breaches of data protection, adhere to recommendations or judgements made by the Information Commissioners Office and will use this information to improve data protection provision and amend the Policy and procedures.	
6	**Consultation**	
6.1	The tenants Policy Review Group has been consulted about the development of this Policy. All OVH staff have been consulted about the development this Policy.	
6.2	The Policy was subject to an external legal review in June 2018.	
7	**Review**	
7.1	This Policy will be reviewed every three years (from the date it is approved) by the Executive Management Team (EMT) and to ensure its continuing suitability, adequacy and effectiveness or as required by the introduction of new legislation or regulation that impacts on the data protection obligations of OVH, changes to OVH business practices or in the light of management system audits.	
8	**Equality Impact Assessment**	
8.1	Was a full Equality Impact Assessment (EIA) required?	No
8.2	When was EIA conducted and by who?	An EIA Relevance Test conducted by the Policy Officer and The Policy and Strategy Manager in 2021 is still relevant to this Policy review.

8.3	**Results of EIA**	The Relevance Test did not indicate there are any differential or adverse impacts for any group with protected characteristics as a result of the operation of this Policy.
9	**Scheme of Delegation**	
9.1	**Responsible committee for approving and monitoring implementation of the policy and any amendments to it**	OVH EMT
9.2	**Responsible officer for formulating policy and reporting to committee on its effective implementation**	Group Director- Governance and Compliance
9.3	**Responsible officer for formulating, reviewing and monitoring implementation of procedures**	Group Director- Governance and Compliance

10	**Amendment Log**		
Date of revision:	**Reason for revision:**	**Consultation record:**	**Record of amendments:**
7th June 2017	Additions made to Policy to reflect current operational practice	See section 6 above	Inclusion of provisions for sharing information that is in the 'public interest'. Inclusion of arrangements for mental capacity assessments where required.
24th July 2018	In line with the introduction of revised Data Protection Legislation.	See section 6 above	Policy updated throughout to include relevant provisions to meet the requirements of UK GDPR and the Data Protection Act 2018.
21st September 2021	In line with the Review Schedule	See section 6 above	There are no significant changes to the Policy in this review.