Data Protection Policy

Regulation and Legislation	This policy links to: • The UK General Data Protection Regulation (UK GDPR); • The Data Protection Act 2018 (DPA 2018); • The Privacy and Electronic Communications Regulations 2003 (PECR); • The Computer Misuse Act 1990 (CMA); • The common law duty of confidentiality; • Any other laws and regulations relating to the protection of personal data.
Approved by	Director of Business Assurance – 1 December 2021
Supporting documents	Subject Access Request Procedure; Data Breach Procedure; Data Subject's Rights Procedure; Email Retention Policy; Tenancy Services CCTV Policy and Procedure; Facilities CCTV Policy and Procedure
Scope	This Policy outlines the key principles in handling personal data and should be followed in conjunction with the relevant procedures and linked policies as detailed above. This policy applies to all Orbit customers and employees.
Reference to "Orbit" means Orbit Group which consists of Orbit Group Limited, Orbit Housing Association Limited, Orbit Homes (2020) Limited, Orbit Treasury Limited and Orbit Capital Limited.	

1. Introduction

1.1 This Policy outlines Orbit's approach to Data Protection. We recognise the importance of protecting the personal data we are entrusted with, and complying with relevant legislation, including:

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018 (DPA 2018)
- The Privacy and Electronic Communications Regulations 2003 (PECR)
- The Computer Misuse Act 1990 (CMA)
- The common law duty of confidentiality
- Any other laws and regulations relating to the protection of personal data.

2. Policy Statement

Orbit is committed to ensuring that:

2.1 All personal data is processed in keeping with the data protection principles in the GDPR, including being: processed lawfully, fairly and in a transparent manner; processed only for specific, explicit and legitimate purposes; adequate, relevant and accurate; not kept longer than is necessary; processed securely; and that wecan demonstrate our accountability and compliance with legal requirements;

2.2 Data subjects' rights around how their data is handled are upheld and can be exercised by data subjects;

2.3 Data sharing is carried out in a safe and secure manner, and in keeping with the principles and data subjects' rights;

2.4 Data is not transferred outside of the European Union (EU) except for in exceptional circumstances where necessary for key service delivery.

2.5 Any data security breaches are reported and managed appropriately.

3. Data Protection Definitions

3.1 Personal data is any information relating to a natural (living) person who is either identified or identifiable. This includes but is not limited to our customers, colleagues and anyone else we come into contact with.

3.2 'Special categories' of personal data includes information about a person's: race or ethnic origin; political opinions; religious or similar beliefs; trade union membership; physical or mental health; genetic and biometric data; sexual life or sexual orientation.

3.3 Other personal data such as bank details may be considered 'sensitive' but will not be subject to the same legal restrictions as the data listed in the special categories above.

3.4 Information about criminal proceedings or offences is regarded as a separate type of personal data, subject to strict legal restrictions.

3.5 Processing means anything that can be done to personal data, including but not limited to, collecting, storing, using, sharing and disposing of data.

3.6 A Data subject is the person to whom the personal data relates.

3.7 A controller determines the reasons for which personal data is collected, and the ways thatit will be processed.

3.8 A processor is an organisation who is responsible for processing personal data on behalf of a controller. For example, a supplier of web-hosted software that the controller uses to hold personal data in, or a repairs contractor who needs to receive customer names and addresses to be able to carry out the repairs.

3.9 The Information Commissioner's Office, or ICO, is the UK's data protection regulator. The ICO produces guidance on how to implement good data protection practices and can take action when a breach of data protection law occurs.

4. Data Protection by 'Design and Default'

4.1 When we are planning projects or new ways of working that involve or affect our processing of personal data, we will consider the data protection implications, and how to ensure we meet legal and good practice requirements, from the planning stages.

4.2 One way we will do this is using Data Protection Impact Assessments (DPIAs), for particularly high-risk processing, The Information Governance's advice will be sought when carrying out DPIAs. The Data Protection Officer will provide advice, approve DPIAs and document the decision process and decisions made.

5. Data Protection Principles

5.1 **Fair, lawful and transparent processing:** Processing of personal data is lawful when the purpose for the processing meets one of the relevant legal conditions listed in Article 6 of the GDPR:

a) Consent of the data subject;
b) Necessary for a contract with the data subject;
c) Necessary for us to comply with a legal obligation;
d) Necessary to protect someone's 'vital interests' ('life or death');
e) Necessary for the performance of a task in the public interest, and the task has a clear basis in law;
f) Necessary for us to pursue our legitimate interests, or the legitimate interests of another organisation, unless the interests are overridden by the interests, rights and freedoms of the data subject.
g) Necessary for preventive or occupational medicine or provision or management of health or social care or treatment
h) Necessary for public health reasons such as reporting contagious diseases to the relevant authorities
i) Necessary for archiving or statistics in the public interest or for scientific or historical research

5.2 To rely on this condition a three-part 'legitimate interests test' should be carried out to show:

1. there is a legitimate interest
2. the processing is necessary to achieve it
3. it does not override the interests, rights and freedoms of the individuals involved

5.3 Where none of the other conditions are met, the **consent** of the data subject is obtained for the data processing.

5.4 Where special categories of personal data are being processed, this is lawful when the purpose also meets one of the legal conditions listed in Article 9 of the GDPR.

5.5 Where none of the other conditions are met, the **explicit consent** of the data subject is obtained for the data processing.

5.6 To be lawful, fair and transparent, our data processing is explained in a Privacy Notice, that includes information about:

- Our identity and contact details and those of our DPO; the reasons and legal basis for processing personal data; explain the legitimate interests pursued, where applicable; the consequences to data subjects of not providing data needed for contractual or statutory reasons; any automated decision making or profiling; who we share the data with; if we send any data outside of the UK and EU, the fact we do this, and any safeguards in place; how long the data is stored; and the legal rights that individuals have around their data, including the right to withdraw consent and to complain to the ICO.

5.7 A short Privacy Notice paragraph is communicated with data subjects at the time of collecting their data, or within one month of receiving their data from a third party, and our full Privacy Notice is on our website: www.orbit.org.uk/privacy

5.8 **Purpose limitations:** We only use the data we collect for the reasons we have explained at the time of collecting the data, in our privacy notice. If we need to use it for another reason, we will assess whether it is compatible with the original reason and inform data subjects about the new reason before further processing.

5.9 **Data limitations:** We minimise the amount of data that we collect and process, restricted to only what is necessary for the reasons we are collecting it. We will not collect or keep any personal data “just in case”.

5.10 **Data accuracy:** We endeavour to ensure the data we collect, and hold is accurate, and kept up to date as appropriate.

5.11 **Storage Limitation:** We will only keep personal data for as long as is necessary for the reasons for which we are processing it, and we will be transparent with our data retention schedules.

5.12 **Confidentiality and Integrity:** We use both technical and organisational security measures to protect the integrity of personal data, including protecting data from unauthorised or unlawful processing, or from accidental loss, destruction or damage. Security measures are appropriate to the level of risk involved in the data and the processing. Measures include, but are not limited to: Systems security; encryption; business continuity plans; physical security of our premises and data; policies; procedures; training; audits and reviews.

5.13 Personal data should not be sent to or from employees personal accounts – email, Facebook Messenger, WhatsApp, etc. – only from Orbit accounts, which are subject to Orbit’s security.

5.14 Orbit has the right to access information on employees work emails and drives so no

personal non-work information should be in Orbit emails or drives.

5.15 Any suspected misuse of Orbit equipment, including emails and internet may be monitored and could lead to disciplinary action being taken.

5.16 More information on Security is in the Information Security Policy.

5.17 Accountability:

To demonstrate and support our compliance with data protection legislation we;

- keep records of the processing we carry out
- have appropriate policies and procedures in place
- train all our colleagues in Data Protection,
- have a Data Protection Officer in post,
- carry out regular audits and reviews of our activities,
- report and investigate data security breaches.

Records of processing include information about how and why we are processing personal data, what data we hold, and the legal basis for the processing, as well as any third parties the data is shared with, including any transfers outside of the EU, and the safeguards in place if data is transferred outside the EU.

6. Data Subjects' Rights

6.1 We process personal data in line with the rights of data subjects' under data protection legislation, including their right to:

- Be informed about their data being processed;
- Request access to their data that we hold;
- Ask for inaccurate data to be rectified;
- Request their data is erased
- Restrict processing of their data, in limited circumstances;
- Object to the processing, in some circumstances, including stopping their data being used for 'direct marketing';
- Data portability, which means to receive copies of some of their data in a format that can be easily used by another organisation or person;
- Not be subject to automated decision making or profiling that has legal or similarly significant effects on them;

6.2 We will respond to, and fulfil, all valid requests as soon as possible, and at the latest within one calendar month, unless we can legally extend the timescale. This can be extended by up to two months in some circumstances.

6.3 Consent

6.3.1 When we rely on consent to process data, Orbit will ensure requests for consent are clear, specific, not bundled together, use opt-in rather than opt-out methods, and will keep evidence

of consent being obtained. We will name any third parties who will rely on the consent and ensure people can easily withdraw their consent. Where consent is withdrawn this must be acted on **immediately**, not within a month as with other requests.

7. Data Sharing

7.1 **Data Processors:** Contractors who will or could process personal data as part of the work they are doing on our behalf are 'data processors'. When working with data processors we will carry out appropriate due diligence checks to ensure that they can provide sufficient guarantees that they will comply with data protection legislation, including keeping data secure and cooperating with us to uphold data subjects' rights.

7.2 **Not all suppliers/contractors** will be 'data processors' – it will depend on what work they are doing, and the nature of the work, and a number of factors that determine who controls the data. Sometimes contractors who handle personal data as part of the work they do for Orbit will be Controllers in their own right regarding the data. In this case, the contract needs different clauses. See the IG Team for more information if you think a contractor is actually a Controller rather than a 'Processor.'

7.3 We will appoint data processors on the basis of a legally binding, written contract, that requires them to, amongst other things: Only process personal data based on our instructions; keep the data secure; assist us to comply with our legal obligations and uphold data subjects' rights; delete or return the data at the end of the contract; and allow inspections and audits of their processing activities.

7.4 Data Processor contracts, and compliance, will continue to be monitored throughout the contract period.

7.5 **Third Parties:** Personal data will only be shared with any other third parties, including other data controllers such as other agencies and organisations, when the sharing has one or more appropriate legal bases, and is carried out in keeping with the data protection principles and while upholding the rights of data subjects.

7.6 There will be situations where we want to share data with organisations who we **work alongside**, but they are not doing paid work for Orbit. For example, other Housing Associations, local charities, social services, housing benefit departments, Police, etc.

7.7 As with all sharing, the sharing must always be assessed against the relevant data protection principles and we must identify the **legal condition** that the reason for the sharing meets, as well as only share the minimum information, and share it securely. Orbit's Privacy Notices should cover this type of sharing, for transparency, but it will not always be appropriate to tell individuals at the time about specific sharing, for example if it would prejudice a police or social services investigation.

7.8 Non-EU data transfers

Personal data will not be transferred outside the European Union (EU) unless it is permitted by one of the conditions in Chapter V of the UK GDPR. This includes storage on cloud-based servers located outside the EU.

8. Data Security Breaches

8.1 All data breaches should be reported immediately to the Data Protection Officer or Information Governance Team (informationgovernance@orbit.org.uk)and will be investigated appropriately, and corrective and preventive action taken.

8.2 Specifically, any personal data security breaches that are likely to result in a risk to data subjects will be reported to the ICO within 72 hours of Orbit becoming aware of thebreach.

8.3 Where a security breach causes a high risk to data subjects, we will also inform the data subjects, without undue delay, to allow them to take any appropriate action that may help to protect them and their data.

9. Roles and Responsibilities

9.1 All colleagues are responsible for reading and understanding this policy before carrying out tasks that involve handling personal data, and for following this policy, including reporting any suspected breaches of it to Orbit's Information Governance Team (informationgovernance@orbit.org.uk) and the Data Protection Officer.

9.2 Individuals may be liable for prosecution for serious breaches of the Data Protection Act 2018, including obtaining, disclosing or retaining data without the consent of Orbit; knowingly or recklessly re-identifying people from anonymised personal information; preventing disclosure of any information an individual has a right to under the Subject Access Right. Any action which breaches this policy will be regarded as being "without the consent ofOrbit."

9.3 All leaders are responsible for ensuring their team read and understand this policy before carrying out tasks that involve handling personal data, and that they follow this policy, including reporting any suspected breaches of it to Orbit's Data Protection Officer and Information Governance Team (informationgovernance@orbit.org.uk)
It is particularly important that the policy is followed when planning any new processes, or changes to processes, that involve personal data.

9.4 Our Data Protection Officer is responsible for advising Orbit and our colleagues about our legal data protection obligations, dealing with breaches of this policy, including suspected breaches, and monitoring compliance with this policy.

9.5 **Training:** Mandatory Data Protection training is required to be completed as part of the induction process. Refresher Data Protection training will be provided annually for all staff. Bespoke training will be provided for

10. Performance Controls and Business Risk

10.1 Compliance with this policy will be monitored by Information Governance as part of a rolling annual Assurance Programme and the ICO Accountability Framework model

10.2 Performance in the delivery of the service will be assessed by Information Governance and Internal Audit

10.2 Performance will be shared through SMT monthly and ARAC as required where risks are identified

10.3 Orbit will carry out a fundamental review of this policy every three years or sooner subject to legal, regulatory changes or if internal changes require it.

11. Essential information

11.1 All Orbit policies and procedures are developed in line with our approach to the following, data protection statement, equality diversity and inclusion (EDI) approach, complaints and customer care policy and our regulatory and legal obligations to ensure we deliver services in a lawful manner and treat people equally and fairly. Orbit's privacy policy can be accessed on our website www.orbitcustomerhub.org.uk/publications/policies/

EA	Equality Analysis was completed on 01/12/2021 and is available to view.
DPIA	A DPIA was approved on 01/12/2021 and is available to view.
Consultation	**Internal:** Information Governance
	External: N/A
Applies to	All Orbit Employees

Document control

Status	Date Issued	Version	Revision
Approved	June 2022	v2.1	

Uncontrolled if Printed

Title	Data Protection Policy		ID103
Doc Type	Policy	Review Cycle	3 Yearly
Circulation	All Departments	Classification	Public / Private

Doc Level 2

Author	Gary Breen	Sponsor	Aman Jhawar
Team	Information Governance	Department	Business Assurance

Directorate Corporate Services

		Date
Approved by	Orbit Group Board	May 2018
Last review	Director of Business Assurance	Nov 2021 Jun 2022
	Next Review (or sooner if changed)	Jun 2025

Revision History

Version Number	Date	Comments / Reason for revision
v1.0	May 2018	Policy revised in line with GDPR requirements
v2.0	Nov 2021	Full three-year review. No change to policy. Following amendments made: 6.1 – added request their data is erased 7.2 – added 7.6 – added 7.7 – added
v2.1	May 2022	5.1 – g-i added 5.2 – added 5.14 – added 5.15 – added 9.2 – expanded