Document Title	Data Protection Policy
Version	FINAL V.3
Release Date	August 2018
Review Date	August 2021
Extension Reason(s)	N/A
Extension date approved	N/A
Approver details	N/A
Document Type	Policy
Sponsor	Aman Jhawar, Business Assurance Director
Author	Clare Paterson

ORBIT

DATA PROTECTION POLICY

Executive Summary	This document outlines Orbit's Data Protection Policy and links to the following Policies and Supporting documents: • Information Security Policy • Privacy Notice • Process for Data Protection Breach • Process for Subject Access Requests • Record Retention Process • Data Protection Impact Assessment It provides a framework within which all handling of personal data will be managed.
Approved by	ET – May 2018 Orbit Group Board – June 2018
EA completed	An Equality Analysis was completed and was low scoring. The key aim of data protection is to treat people fairly and lawfully with regards to how their data is processed, which includes avoiding discrimination and this policy supports that, as well as demonstrating inclusivity.
Explain how customers have been involved.	Customers have not been involved in the formulation of this policy as it is based on legal requirements and their influence in policy formulation would be minimal. They have been consulted on general understanding of the policy and its delivery.
Consultation	All areas of the business will be impacted and as such a rolling programme of awareness and workshops have been delivered to all areas of the business.
Applies to	All staff (including temporary staff, consultants and Board members)

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 in the Executive Summary.

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 General Data Protection Regulation (GDPR);
- The Privacy and Electronic Communication Regulation (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.

1.2 In particular, Orbit is committed to ensuring that:

1.2..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;

1.2..2 We can demonstrate our accountability and compliance with legal requirements;

1.2..3 Data subjects' rights around how their data is handled are upheld and can be exercised by data subjects;

1.2..4 Data sharing is carried out in a safe and secure manner, and in keeping with the principles and data subjects' rights;

1.2..5 Data is not transferred outside of the European Union (EU) except for in limited circumstances.

1.2..6 Any data security breaches are reported and managed appropriately.

2. RESPONSIBILITIES

2.1 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 Data Protection Officer.

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. Any action which breaches this policy will be regarded as being "without the consent of Orbit."

2.2 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.
It is particularly important that the policy is followed when planning any new processes, or changes to processes, that involve personal data.

2.3 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.

3. TRAINING AND GUIDANCE

3.1 Mandatory data protection training will be provided at least annually for all staff

3.2 Further information is provided in policies and procedures linked to this policy, and extra guidance may be issued through other communication channels as and when required.

4. DATA PROTECTION IN PRACTICE

4.1 Definitions

4.1.1 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.

4.1.2 '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.

4.1.3 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.

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

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

4.1.6 Data subject is the person the personal data relates to.

4.1.7 A controller determines the reasons for which personal data is collected, and the ways that it will be processed.

4.1.8 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.

4.1.9 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.

4.2 'Privacy by Design'

4.2.1 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.

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

4.3 Data Protection Principles

4.3.1 **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.

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

4.3.3 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.

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

4.3.5 To be 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 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.

4.3.6 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

4.3.7 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.

4.3.8 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".

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

4.3.10 Data retention: 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.

4.3.11 Data security & 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.

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

More information on Security is in the Information Security Policy.

4.4 Data subjects' rights

4.4.1 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;
- 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;
- Withdraw consent when we are relying on consent to process their data.

4.4.1 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.

4.4.2 All electronic 'direct marketing' is subject to the Privacy and Electronic Communications Regulations (PECR) which requires that we obtain consent before sending unsolicited electronic direct marketing messages.

4.5 Accountability

4.5.1 To demonstrate and support our compliance with data protection legislation, we keep records of the processing we carry out, we have appropriate policies and procedures in place, we train all our colleagues in data protection, we have a Data Protection Officer in post, we carry out regular audits and reviews of our activities, and we report and investigate data security breaches.

4.5.2 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.

4.6 Data sharing

4.6.1 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.

4.6.2 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.

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

4.6.4 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.

4.6.5 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 GDPR. This includes storage on cloud based servers located outside the EU.

4.6.6 Data security breaches: All breaches of this policy should be reported immediately to the Data Protection Officer, and will be investigated appropriately, and corrective and preventive action taken.

4.6.7 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 the breach.

4.6.8 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.

5. EQUALITY AND DIVERSITY

5.1 Orbit policies are developed in line with our Equality and Diversity policy

6. PRIVACY STATEMENT

6.1 Orbit are collecting information ('personal data') so that we can manage and support our relationship with our customers, comply with legal obligations, improve our services and achieve our legitimate business aims. We are committed to complying with data protection legislation when handling customers' data. Customers have rights around their data, including the right to access their data, and to object to the way it is processed. For more information on how and why we process customers' data, and how customers can exercise their rights, please see our full Privacy Policy on our website at www.orbit.org.uk/privacy-policy/.

7. MONITORING AND ACCOUNTABILITY

7.1 Compliance with this policy will be monitored by the Business Assurance Director, supported by reviews undertaken by internal audit. The success of this policy will be measured through compliance with Orbit's risk appetite which was approved by the Board in March 2018.

8. REVIEW

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