Onward
Creating positive spaces

Data Protection Policy

1. Aim

1.1 This Data Protection Policy provides guidance for all Onward employees & Board Members on Data Protection issues to be considered when handling personal information and data.

1.2 Onward needs to collect, process and store personal information about tenants, employees, suppliers and other business contacts in order to carry out its business and provide its services. This information may include name, address, email address, date of birth, personal and sensitive personal details. In addition, we may occasionally be required to collect and use certain types of such personal information to comply with the requirements of the law. No matter how it is collected, recorded and used (e.g. on a computer or on paper) this personal information must be dealt with properly to ensure our compliance with the General Data Protection Regulation (GDPR) and UK Data Protection Bill 2017.

2. Scope

2.1 GDPR regulates the processing of information relating to identifiable living individuals, including obtaining, retaining, use or disclosure of such information.

2.2 The lawful and proper treatment of personal information by Onward is extremely important to the success of our business and to maintain the confidence of our service users and employees. OH must ensure it treats personal information lawfully and correctly, and it is our policy to comply with the seven principles of GDPR.

2.3 All Onward staff & Board Members must abide by this Policy and associated standards and procedures.

2.4 The Policy relates to all hard copy documents and electronic records.

3. Policy detail

3.1 Information Classification

Onward will operate on the principal that all information we store and manage falls into one of the following categories:

Confidential – Information which relates to our business, not people, which we do not want to be released outside of the organisation. This could include financial information, details of our IT network or commercially sensitive information about our plans to grow as an organisation;

Personal information – Information about any living individual which is able to identify that specific person;

Sensitive personal information – Information about a living individual which meets the criteria defined in the GDPR as 'special categories' including ethnicity, sexuality, religious beliefs, criminal record etc.;

General information – Any information which does not fall into any of the other 3 categories listed above

3.2 Onward will ensure that standards and procedures will be available to provide sufficient clarity to employees regarding how to implement this policy in practice.

3.3 Onward will provide all staff with regular awareness training on Data Protection and Information Security. Initial training will be undertaken for all new employees as part of any induction programme. Upon completion new employees will be required to sign a declaration of understanding and agree to comply with this Data Protection Policy.

3.4 Onward will provide clear lines of report and supervision for compliance with GDPR.

3.5 Employees through appropriate training and responsible management will observe all forms of guidance, codes of practice and procedures about the collection, processing, storage and sharing of personal and sensitive personal information, and ensure all information is destroyed in accordance with GDPR requirements and Onward's Information Retention Policy.

4. Responsibility and monitoring

4.1 Onward will appoint a Data Protection Officer, who will have overall responsibility for Data Protection, whose role profile and description will meet requirements set out in the GDPR.

4.2 As a business, and employer, Onward has a number of legal responsibilities. In order to protect the business and ensure compliance, Onward needs to monitor ICT Network and System activity, and investigate any issues arising.

4.3 Whilst Onward will not access employee data without good reason, no user should have any expectation of privacy as to his or her communications or data storage. Specific messages may be opened and interrogated, where there is sufficient justification under the Employment Practices Data Protection Code, and where this is permitted under the relevant legislation.
4.4 In conducting routine communication system reviews, such as email and chat, Onward ICT will normally only analyse logs and header information such as sender and recipient, date and subject.

4.5 Where an investigation is undertaken, this will be conducted within the boundaries of the relevant statutes and best practice guidance (for example, The Employment Practices Data Protection Code: Monitoring at Work). This Code prevents covert monitoring except in exceptional circumstances, such as where there is reason to believe this policy is being deliberately contravened. This will normally be where colleagues or management have reported internet abuse, where our monitoring software has identified potential non-compliance, or through the presence of questionable data within our systems.

4.6 Onward reserves the right to inspect any and all files stored in any area of the business, including networked and non-networked equipment and storage devices, where we have reason to believe that an individual may have contravened the terms of this Policy.

4.7 Onward undertakes that any review of user access data will only be undertaken where there are reasonable grounds to believe this policy has been contravened. Where there is evidence of criminal activity, OH will hand over information to relevant law enforcement authorities, and will cooperate fully with any subsequent investigations intended to prevent and/or detect crime.

4.8 Onward takes the misuse, loss or misappropriation of information very seriously. Breach of our Data Protection and Security policies by colleagues may result in disciplinary action up to and including summary dismissal, consistent with Onward's Disciplinary procedure, and for contractors or agents in termination of contract.

Linked documents:	Information Security – All Users Policy ICT Security Policy PCI DSS Credit Card Security Policy Information Retention Policy Freedom of Information Policy

Date implemented:	12 March 2018
Policy lead:	Gary Williams, Data Protection Officer, Business Assurance
Approved by:	Senior Leadership Team
Approved on:	12 March 2018
Next review date:	March 2020

Reference number:	DP01
Version:	1
Document replaces:	Symphony Data Protection policy 2015