Data Protection & Privacy Policy

Version Control

Amendments to this document are detailed below

Version Number	Date Amended	Comments	Date Approved	Author	Approved by
1.0	10/11/2017		11/12/17	Chris Down	C&R
1.1	14/12/17		21/12/17	Chris Down	A&R
1.2			30/01/18	Chris Down	Board

Merlin

Purpose:

The purpose of our Data Protection & Privacy Policy is to set out how Merlin will ensure that personal data relating to our customers, staff and other data subjects is:-

a) processed lawfully, fairly and in a transparent manner in relation to individuals;
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
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;
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;
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.

The above sets out Merlin's main responsibilities under UK data protection law which is derived from the EU's General Data Protection Regulation (GDPR). Additionally, `Merlin is responsible for, and must be able to demonstrate compliance with the principles relating to the processing of personal data.

Scope:

The principles and terms within this policy apply to all information and documentation held by Merlin which relates to personal data.

Personal data is defined as any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address.

The GDPR's definition of personal data is more detailed than the Data Protection Act 1998 (DPA), and makes it clear that information such as an online identifier – e.g. an IP address – can be personal data. The more expansive definition provides for a wide range of personal identifiers to constitute personal data, reflecting changes in technology and the way organisations collect information about people.

Merlin

Policy Statement & Principles:

Policy Statement

We are committed to a 'Privacy by Design' approach to personal data which is consistent with our values.

Our Values	Our Privacy by Design Principles
We start with our customers and work backwards	We believe in privacy by default and we embed privacy into design
We're open, honest and keep our promises	We believe in visibility and transparency and are committed to end-to-end security
We aim high	We are proactive not reactive, preventative not remedial. We won't trade privacy off against other objectives
We value people and work together	We respect user privacy

Our commitment to 'Privacy by Design' also aligns with the six pillars of our customer experience strategy:

We are committed to Privacy by Design because we understand that we are accountable for what we do and for what we should do. This includes ensuring that we protect our customers, staff and other data subjects right to privacy.

Policy Principles

As part of our commitment to Privacy by Design we adopt the following principles:

We believe in privacy by default and we embed privacy into design

Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data is automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy − it is built into the system, by default.

Privacy by Design is embedded into the design and architecture of our IT systems and business practices. It is not bolted on as an add-on, after the fact. As a result privacy is an essential component of the core functionality being delivered. Privacy is integral to our systems processes and practices, without diminishing functionality.

Managers and staff must consult the data protection officer were a change to the way we use personal data could introduce new privacy risks in data processing activities. This is possible when new data processing processes, systems or technologies are introduced or when data is bought from third parties.

We believe in visibility and transparency and we're committed to end-to-end security

Visibility and transparency are essential to establishing accountability and trust. Privacy by Design seeks to assure all stakeholders that whatever the IT system or business process or involved, it is in fact, operating according to stated promises and objectives, subject to independent verification.

Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire data lifecycle. Strong security measures are essential to privacy, from start to finish. This ensures that all data is securely retained, and then securely destroyed when no longer required in a timely fashion. Privacy by Design ensures secure lifecycle management of information, end-to-end.

We are proactive not reactive; preventative not remedial. We won't trade off privacy against other objectives

Our Privacy by Design approach is characterised by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. Our Privacy by Design approach does not wait for privacy risks to materialise, and it aims to prevent data protection incidents from occurring. In short, Privacy by Design comes before-the-fact, not after.

Privacy by Design seeks to accommodate all legitimate interests and objectives in a win-win manner. Privacy by Design avoids unnecessary trade-offs, such as privacy vs. security, demonstrating that it is possible, and far more desirable, to have both.

We respect user privacy

Above all, Privacy by Design requires us to keep the interests of the individual uppermost by offering measures such as strong privacy defaults and respect for data subject's rights.

Merlin has nominated a Data Protection Officer as described by the GDPR. The appointment of a Data Protection Officer is not mandatory for the Housing Sector but Merlin sees the role of the Data Protection Officer as important in delivering our Privacy by Design approach and ensuring compliance with data protection law.

Additionally, we recognise that we process a significant volume of sensitive data, for example related to our customer's health, as part of our core business.

Responsibilities:

Merlin is responsible for, and must be able to demonstrate compliance with the principles relating to the processing of personal data.

.

The Board has overall responsibility for this policy and is committed to Privacy by Design.

The annual declaration signed by members of Merlin's Board includes an acknowledgement of an absolute duty of confidentiality to Merlin. This states that Board members must not disclose to any third party any confidential information which they have obtained because of their position on the board

The Audit & Risk Committee will obtain assurances relating to the adequacy and effectiveness of risk, control and governance processes relating to data protection and privacy in Merlin.

The committee will receive reports on Merlin compliance with the principles of this policy data protection law.

The Data Governance Group / Corporate & Risk Panel will maintain and monitor proper arrangements for data risk management, ensuring these are effectively developed, implemented, managed, monitored and embedded across Merlin. The Corporate & Risk Panel will ensure that proper arrangements for risk management and internal control are maintained and monitored in Merlin's approach to data protection and privacy. Ensuring these are effectively developed, implemented, managed, monitored and embedded across Merlin.

Heads of Service and Line Managers are responsible for ensuring that all staff in their teams understand the Privacy by Design policy statement and principles and the underlying procedures and guidance. Heads of Service and Line Managers must also encourage the reporting of data protection incidents as part of a commitment to continuously improving standards of data protection and privacy.

All Staff are required, by the Employees Code of Conduct to abide by procedures designed to protect the confidentiality of information held about residents, customers or other employees.

The Data Protection Officer is responsible for the following tasks:

- To inform and advise Merlin and its employees about their obligations to comply with the GDPR and other data protection laws;
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advising on data protection impact assessments; train staff and conduct internal audits; and
- To be the first point of contact for supervisory authorities (the Information Commissioner's Office) and for individuals whose data is processed (employees, customers etc.).

In particular the Data Protection Officer is responsible for ensuring that appropriate procedures and guidance on our approach to data protection and privacy are available to Board members, managers and staff.

Our data protection and privacy procedures will set out a specific way to carry out a specific duty or activity. These will include a clear desk procedure; procedures for carrying out data protection / privacy impact assessments and procedures for complying with data subject's rights under the GDPR.

Performance Standards / Measures of success:

The following performance standards and measures of success have been identified.

- All staff confirm that they have read and understood this policy;
- Data protection and privacy training is delivered to all staff as required by our data protection and privacy training programme;
- Number of data protection incidents is reduced year on year;
- Number of significant data protection incidents (defined as incidents that merit reporting to the Board) and data protection breaches (defined as incidents that merit reporting to the ICO) is reduced year on year;

Diversity, Equality and Inclusion

This policy operates in tandem with the Societies wider Equality and Diversity policy which prohibits discrimination on the grounds of disability, age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation.

Customer Insight – Understanding our Customers

To help us understand our customers we collect special categories of data and information about lifestyle relating to our customers.

We minimise use of this data but, given the services we provide there are times when we may have a legitimate interest in processing this data. We may therefore ask customers to consent to the collection and processing of this data. We will always give a ‘prefer not to answer’ option when we for lifestyle or special categories of data.

This policy has taken into account that there is an imbalance of power (as defined by the Information Commissioner’s Office) between Merlin, as landlord, and our customers and prospective customers, as tenants or future tenants. This Data Protection & Privacy Policy, together with other key policies and procedures relating to privacy, confidentiality and document retention, helps redress the imbalance of power by ensuring that data subjects’ rights are respected.

Assurance Framework

Heads of Service will be asked to ensure that this policy is communicated to all staff in their teams and a copy of the policy will be made available via the Portal. Awareness of our Data Protection & Privacy Policy will be reinforced on a periodic basis via news items on the Portal, training and team talks.

The Data Governance Group / Corporate & Risk Panel provide assurance to the Board and Audit & Risk Committee (A&R) in discharging their responsibilities for ensuring the

adequacy and effectiveness of data risk management across Merlin. The group will escalate matters, provide recommendations and regularly report to C&R, A&R and/or Board.

The Audit & Risk Committee is responsible for obtaining assurances relating to the adequacy and effectiveness of risk, control and governance processes relating to data protection and privacy. The committee will also review material data protection and privacy incidents, risk exposures or control failings

Risks

Adherence to this policy helps mitigate the following risk:

“Data is amended, disclosed or withheld inappropriately or without proper authorisation leading to breaches of data protection law”.

Further information

Please refer to the Privacy and Data Protection section of Mint for relevant procedures and guidance.

Document details

Owner:	Chris Down – Data Protection Officer
Approval:	Board
Next review:	January 2019

Merlin

Appendix 1 – Supporting Procedures & Guidance

Name of Document	Owner	Status	Approval By & Target Date
Procedures			
Data Protection Incident Reporting Procedure	DPO	Draft produced, reporting template, scoring mechanism and log in use. DGG feedback to be sought	DGG 11/17
Incident Management Process	Head of IT	DP content added and Approved	C&R 10/17
Procedure for Verifying Identity of Callers	Head of Customer Experience	Draft produced, Nicola Noah finalising	H&CLT TBC
Cardholder not Present Procedure	Head of Customer Experience	Checking position with Nicola Noah.	H&CLT 12/17
Data Porting Procedure	Head of IT	Technical guidance needed on complying with data subject rights	F&RLT 2/18
Procedure for Restricting Access to Data	Head of IT	Technical guidance needed on complying with data subject rights	F&RLT 2/18
IT Disaster Recovery Procedure	Head of IT	Included within BCP which is being updated	C&R TBC
Subject Access Request Procedure	DPO	This guidance exists but needs to be updated	DGG 4/18

Merlin

Name of Document	Owner	Status	Approval By & Target Date
Guidance			
Procuring and Contracting with Data Processors	DPO or Procurement Business Partner	Data processors register is being prepared. Supplier questionnaire drafted (used for 2020); contract clause drafted, procedure about use of questionnaire and clause to be developed.	C&R 1/18
Guidance on Data Subjects Rights	DPO	Draft produced	RSG 1/18
Data Protection Impact Assessment Guidance	DPO	Draft produced	C&R 12/17
Data Sharing Guidance	DPO	Draft guidance on sharing data externally produced.	DGG 1/18
Data Erasure / Deletion, Retention Guidance	DPO	This guidance exists but is currently being updated	C&R 1/18
Guidance on Obtaining and Recording Consent	DPO	Draft produced	DGG 11/17
CCTV Guidance and Code of Practice	DPO	This guidance exists but needs to be updated.	C&R 2/18
Photography Guidance	DPO	Draft produced and shared with Property Solutions, Investment and Customer Experience	DGG 2/18
Data Protection Guidance - Voids	DPO / Repairs and Voids Project Manager	Not started	ILT 2/18

Merlin

Name of Document	Owner	Status	Approval By & Target Date
Data Protection Guidance - Recruitment	DPO / Head of HR	In progress	DGG 1/18
Data Protection Guidance - Red Flag Procedure	DPO / Head of Customer Experience	Not started	H&CLT 2/18
Data Protection Guidance - Insight	DPO / Leader for Diversity, Equality, Inclusion & Partnerships	Risk mitigation guidance has been provided. This will be updated following a Data Protection impact Assessment	H&CLT 2/18