Data Protection, Privacy & Confidentiality Policy

V8.0

Aster Group is the overarching brand name of Aster Group Ltd and all of its subsidiaries

1 Scope

1.1 This policy sets out the Aster Group's approach to ensure compliance with the UK General Data Protection Regulations (UK GDPR) and the Data Protection Act 2018 (DPA 2018), jointly referred to in this policy as 'UK GDPR & DPA 2018'.

1.2 Entities within the Aster Group are Data Controllers of the personal data they collect and process as defined by UK GDPR & DPA (2018). Registration will be maintained with the appropriate regulatory body (currently the ICO) for all entities within the group acting as a data controller. We will publish these registration numbers on our website.

1.3 Entities within the Aster Group may also act as a Data Processor.

1.4 This policy applies to all personal data and special category personal data processed by entities of the Aster Group, and hereafter 'Aster Group' refers to all entities individually and collectively. Where appropriate and with a lawful basis for doing so, data will be shared within the Aster Group.

1.5 Personal data is defined as any information related to a natural (living) person or 'data subject' that can be used to directly or indirectly identify the person.

1.6 To deliver its purpose as a landlord, service provider, developer, employer and charitable organisation, Aster Group needs to collect and process personal data. This could include information about customers, neighbours, close friends and family of customers and service users, potential customers, colleagues, employment applicants, board members, suppliers and others with whom it communicates.

1.7 The lawful and ethical treatment of personal data by Aster Group is extremely important to the success of our business and to maintain the confidence of our customers, colleagues and other stakeholders.

1.8 The duty of confidentiality also extends to any sensitive commercial information relating to Aster Group or its associates.

1.9 This policy forms part of an enabling approach to Data Protection, supporting lawful processing and the proportionate and legitimate use of and sharing of information to achieve positive outcomes and deliver good services.

2 Policy Statement

2.1 Aster Group is committed to protecting the rights and privacy of individuals in line with the UK GDPR & DPA (2018) and supporting them in exercising these rights.

2.2 We will demonstrate compliance under the Data Protection Principles derived from UK GDPR (Article 5) by ensuring personal data 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; ('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 ('storage limitation');
(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').

2.3 As a Data Controller, Aster Group will be committed to demonstrating compliance with the above principles through its Data Protection framework.

3 Definitions of Personal Data

3.1 Personal data is any information relating to a living person that can be used to directly or indirectly identify that person. Examples of personal data include but are not limited to;

Name, address, contact details	Telephone numbers, email and current, previous and forwarding addresses
Family details	Marital status, next of kin, authorised contact and children
Identification information	Age, date of birth, gender
National identifiers	National Insurance, social security, driving licence or passport number
Financial information	Income, bank account details and benefit entitlements
Economic situation	Employment or education details
Images and recordings	Photographs, CCTV images, films and telephone recordings
Online and device indicators	IP address or cookies, location data

3.2 Special Category personal data or 'sensitive data' as defined under UK GDPR, includes but is not limited to;

- personal data revealing **racial or ethnic origin**
- personal data revealing **political opinions**
- personal data revealing **religious or philosophical beliefs**
- personal data revealing **trade union membership**
- **genetic data**
- **biometric data** (where used for identification purposes)
- data concerning **health**
- data concerning a person's **sex life**
- data concerning a person's **sexual orientation**

Lawful basis for processing personal data

4.1 We must have a lawful basis for processing personal data. The bases available to us are;

- for the **performance of a contract** or to take steps to enter into a contract, *e.g. a tenancy agreement*
- for compliance with a **legal obligation** *(including court orders and the prevention and detection of crime or ASB)*
- to protect the **vital interests** of an individual or another person *(i.e. necessary to protect an individual's life in an emergency)*
- for the performance of a task carried out in the **public interest** or official functions and where this has a clear basis in law
- in the **legitimate interests** of Aster Group or a third party, except where such interests are overridden by the interests, rights or freedoms of the individual
- **consent, where** the individual has given clear consent for us to process their personal data for a specific purpose (which should only be used when a genuine choice can be offered)

4.2 We will record each processing activity and record the lawful basis for each. When a new processing activity arises, we will consider and record the lawful basis before proceeding.

4.3 We recognise that special category data needs more protection and in addition to the above lawful basis we will also ensure we meet one of the below lawful bases for processing, and that we apply additional privacy by design measures where necessary. The lawful bases available to us are;

- **explicit consent** of the individual
- it is necessary for carrying out obligations under **employment, social security or social protection law**
- to protect the **vital interests** of an individual or another individual (must be a matter of life or death)
- it relates to personal data **made public** by the individual
- it is necessary for the **establishment, exercise or defence of legal claims**
- it is necessary for reasons of **substantial public interest** (with a basis in law - this is a complex area and includes matters such as fraud, equalities monitoring, insurance, as examples)
- it is for the purposes of **preventative or occupational medicine**, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services or a contract with a health professional
- for reasons of **public interest in the area of public health** (with a basis in law)
- **archiving, scientific, historical research or statistical purposes** (with a basis in law).

4.4 When relying on a lawful basis which has an additional requirement for a basis in law, we will ensure we also meet the associated basis in law.

4.5 Where we rely on consent for processing, it must be;

- freely given and the individual must be able to change their mind and easily withdraw their consent
- easy to understand, (including additional measures where necessary for vulnerable customers or those with accessibility needs), requiring a positive action to say yes
- separate from other terms and conditions

4.6 Explicit consent relating to special category data must be expressly confirmed in words, rather than by any other positive action.

4.7 Criminal conviction or offences data includes alleged offences or proceedings for an offence committed or alleged to have been committed by an individual. It also extends to personal data relating to victims and witnesses. To process criminal offence data we must ensure it is for a permitted reason. Permitted reasons available to Aster include;

- Employment, social security and social protection
- Health or social care purposes
- Preventing or detecting unlawful acts
- Protecting the public against dishonesty
- Regulatory requirements relating to unlawful acts and dishonesty

5 Sharing Personal Data

5.1 To carry out our business and deliver services, Aster will need to share data with various types of third party. In doing this we will consider and balance the rights of the individuals concerned, public interest and the legal and regulatory interests of Aster and the third parties.

5.2 Examples of appropriate data sharing include;

Permission to Share	The individual has given permission for Aster to share information with others *e.g. family, friends, elected representatives or Power of Attorney (PoA)*
Referrals	The individual has given permission or PoA for Aster to share information with third party support agencies *e.g mediation bodies, charitable organisations*
Multi-Agency working	Where information exchange protocols exist with other agencies for example the Police, Social Services or as part of multi-agency public protection arrangements (MAPPA) or multi-agency risk assessment conference (MARAC) networks
Safeguarding	Co-operating with local authorities implementing their statutory duties around safeguarding
Legislation and Regulation	For example relating to welfare benefit or reduction and prevention of crime and disorder
Contractors or suppliers providing services under instruction from Aster	Providing information to a third party data processor so they can perform a service for us *e.g. a mailing house, IT platform or property maintenance contractor*
Protection of Asters financial interests	Such as ensuring utility companies direct utility charges to those responsible for paying them

5.3 When we discuss personal information, we will take steps to assure ourselves that the person we are talking to is who they claim to be and if not the individual the information relates to, that they have the appropriate authority. Our **Customer Verification Procedure** guides colleagues in how to gain this assurance.

5.4 Requests for personal information made by a representative of the individual will be processed under the **Permission to Share Procedure**. Where we are asked to share information regarding an individual by a representative, confirmation shall be sought from the data subject first.

5.5 We will always share data safely and securely using appropriate technical protection measures. This is further outlined in the **IT Security Policy**.

5.6 Where we share personal data as a Data Controller with Data Processors acting on our behalf, we shall ensure that a Data Processing Agreement is in place.

5.7 Where we are sharing Data with other Data Controllers, *e.g. Local Authorities, Police,* we will where possible adopt County Information Sharing Protocols where these are in place.

5.8 We provide additional information and guidance to colleagues in our **Data Sharing Guidance, Safe Data Transfer Guidance** and **Ad-Hoc Requests Procedure**.

5.9 **NHS National data opt out**

Aster Group reviews its data processing on an annual basis to assess if the national data opt-out applies. This is recorded in our Record of Processing Activities. All new processing is assessed to see if the national data opt-out applies.

At the time of publishing this policy, Aster Group does not share any data for planning or research purposes for which the national data opt-out would apply.

6 Data Retention & Data Minimisation

6.1 We will only store information for as long as is reasonably necessary for us to fulfil the purposes set out in our Privacy Notice. This is typically a maximum of six years after we cease to have a relationship with an individual or if we are in dispute, until legal proceedings have ended, whichever is longer. Data relating to property is typically held for 12 years after interest in a property ceases. Where personal data is held longer than this, this is normally to comply with legal or regulatory requirements. Retention periods for all records will be maintained in the **Aster Group Document Catalogue**.

6.2 We will periodically review whether aspects of data sets can be minimised so individuals are no longer identifiable. Examples of when it would be appropriate to do this include satisfaction surveys, historical schedules of works or housing sales data.

6.3 Our **Good Information Management guidance** sets out Asters approach to disposal or retention of all information and data. Our **Document Catalogue** includes our retention schedule.

7 Information Security & Data Breaches

7.1 We are committed to ensuring the security of information held in our IT systems. and archiving facilities. We will ensure the appropriate investment in our security arrangements and ongoing due diligence. Our **IT Security and Usage Policy** communicates the responsibilities of individual colleagues.

7.2 In the event of an Information Security Event (data breach), we will fulfil our responsibilities as a Data Controller (or Data Processor where relevant) under UK GDPR regarding notification to the supervisory authority (Information Commissioners Office). Our approach to this is set out in our Asters **Information Security Events (Data Breach) Procedure.**

7.3 A personal data breach means the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes, arising from action or inaction. It also means that the term ‘breach’ is wider than the commonly recognised loss or inappropriate sharing of personal data.

Examples include;

Confidentiality breach	Unauthorised or accidental disclosure of, or access to, personal data. Examples include; ▪ Inadvertently verbally disclosing personal data to the incorrect person – over the telephone or, in person ▪ Misdirecting an email or posted letter containing personal data ▪ Copying information off of Aster's IT network, for example to a personal email address ▪ Theft or loss of a laptop or electronic device ▪ Theft or loss of paper documents ▪ Insecure disposal of paper documents ▪ Unauthorised access to paper or IT system records containing personal data, whether internally or as a result of hacking ▪ Indiscreet conversations, resulting in being overheard
Availability breach	Accidental or unauthorised loss of access to, or destruction of, personal data. Examples include; ▪ Cyber-attack ▪ Loss of access to systems for a period of time
Integrity breach	Unauthorised or accidental alteration of personal data. Examples include; ▪ Changing data without verification

7.4 All personal data security incidents (i.e. near misses) and breaches must be reported to the Information Governance team. Asters **Information Security Events (Data Breach) Procedure** provides further guidance.

7.5 All breaches or suspected breaches will be investigated in accordance with this procedure. As required by the UK GDPR, any breach where it is likely to result in a risk to the rights and freedoms of individuals will be reported to the Information Commissioners Office (ICO). We will aim to do this within the required 72 hours' time period of Aster becoming aware of the breach.

7.6 If a breach is likely to result in a high risk to the rights and freedoms of individuals, or concerns individuals with vulnerabilities that may be adversely affected by the breach we will inform those concerned as soon as possible to enable them to take steps to minimise the potential for harm as a result of the breach.

7.7 We require our third party Data Processors (who process personal data on our behalf) to notify us within 24 hours of becoming aware of a data breach.

8 Privacy by Design

8.1 We are committed to privacy by design and will not trade privacy off against other objectives.

8.2 We will carry out a screening assessment and if identified as necessary, a Data Protection Impact Assessment (DPIA) when beginning a new project, making changes to our data processing activities, developing or reviewing a policy or introducing a new technology including the use of generative AI.

8.3 We will maintain a DPIA register.

8.4 Our **DPIA process** and **AI Risk Assessment** support colleagues to consider data protection and deliver the maximum possible privacy by design.

9 Transparency & Data Subject Rights

Privacy Notice

9.1 We will publish a Privacy Notice on the Aster Group website setting out details of our data processing activities including;

- What we collect and why
- Our lawful basis for doing so
- Who we share personal data with in the course of delivering our services
- How long personal information is retained for
- Individual data subject rights and how to exercise them
- How to contact Aster's Data Protection Officer

Data Subject Rights

9.2 We are committed to meeting the rights of individual data subjects under the Act. These rights include;

Individual rights (UK GDPR)	What this means
The right to be **informed**	▪ We must be transparent in our use of their personal data, including an accessible Privacy Notice
The **right of access** to their personal data	▪ An ability to request we provide access to or a copy of the personal data we hold and process, known as a 'Subject Access Request' (SAR).
The right to **rectification**	▪ We must correct inaccurate or incomplete personal data 'without undue delay' when advised of it.
The right to **erasure** (the right to be forgotten)	▪ We must erase personal data 'without undue delay' when it is a valid request and certain conditions apply
The right to **restrict processing**	▪ An ability to suppress or 'block' processing of their data ▪ To insist we store just enough information to meet a purpose but do not actively use it.
The right to **data portability**	▪ When data has been given through consent or performance of a contract, an ability to request and reuse their own personal data
The right to **object**	▪ We must stop processing personal data when certain conditions are met
Rights in relation to **automated decision making and profiling**	▪ The ability to challenge and request a review of any decisions made. These rights are specific to circumstances when explicit consent has been given or when entering into or performance of a contract.

9.3 Our **Individual Data Subject Right Procedure** provides guidance to colleagues.

10 Accountability, Roles & Responsibilities

Data Protection Officer

10.1 The Data Protection Officer (DPO) is the Head of Risk & Compliance. The DPO is not personally responsible for compliance as this is the responsibility of the Data Controller (Aster Group Ltd or a subsidiary) and any Data Processors.

10.2 In summary the DPO's duties are to:

- inform and advise Aster and colleagues about their obligations to comply with data protection legislation
- monitor compliance with data protection legislation, including managing internal data protection activities, train colleagues and conduct internal audits
- provide advice on data breaches, DPIAs and SARs
- be the first point of contact for ICO and Data Subjects
- report to Aster governing bodies.

10.3 When performing these duties, the DPO will have due regard to the risk associated with processing operations, and consider the nature, scope, context and purposes of processing.

10.4 Aster, as Data Controller, must support the DPO and allow them to carry out their legal duties as set out in the Act.

10.5 Aster will take account of the DPO's advice and the information they provide on Asters data protection obligations. Adequate resources will be provided to enable the DPO to meet their data protection legislation obligations, and to maintain their expert level of technical knowledge. If a decision is made at any time not to follow the advice given by the DPO, the reasons will be clearly documented to demonstrate accountability.

10.6 The Information Governance team will carry out the day to day duties on behalf of the DPO and provide data protection advice, guidance and support to Aster Group colleagues. Adequate resources will be provided to enable the IG Team to support the DPO and to maintain their expert level of technical knowledge.

Governance

10.7 The Board of Aster Group Ltd are responsible for ensuring compliance with data protection laws. They are supported in this responsibility by the Group Risk & Assurance Committee.

Leaders & Colleagues

10.8 Leaders in each service area are responsible for;
- Understanding what personal information is held and the uses, access to and data flows of that information
- Ensuring privacy by design when implementing business or policy changes
- Ensuring third party contractors and suppliers adopt a data Processing Agreement
- Understanding and addressing the risks to that information and ensuring it is used in ways that are compatible with the Act.
- Supporting and co-operating with the DPO and IG Team regarding Data Subject Rights and Data Breaches.

10.9 All colleagues are responsible for complying with data protection policy, procedure and guidance and maintaining their knowledge of such.

11 Training & awareness

11.1 We will ensure data protection training is provided to all colleagues. This will be a layered approach including;

- Technical data protection specialists will have access to the training required to ensure their knowledge remains up to date.
- A self-learn e-learning module to be completed by all colleagues within 3 months of joining and repeated annually.

- Colleagues in Supported Employment will receive training via alternative means, tailored to their role and their access needs.
- Role specific training will be delivered such as enhanced customer verification training to contact centre colleagues.
- Regular awareness initiatives will support the formal learning.
- Guidance and 'how to' guides shall be made available to all colleagues.

11.2 The Information Governance Team will provide assurance and support leaders by providing them with Policy and e-learning compliance data for their business area so that training gaps can be addressed.

12 Monitoring & Review

12.1 The effectiveness of this policy will be continuously monitored and the embedding of the policy scrutinised after 12 months by the Operational Scrutiny and Assurance Panel.

12.2 This policy will be reviewed every 3 years unless business need, regulation or legislation prompts an early review.

12.3 Effectiveness of the Policy will also be through;

- Monitoring and reporting on Data Protection e-learning on an annual basis (all colleagues)
- Monitoring and reporting on compliance of reading this policy on an annual basis (all colleagues)
- Frequency, type and service area of data breaches and near misses
- Frequency of Data Subject Rights Requests complied within statutory timescales
- Occurrences of data subject complaints submitted through the Group Complaints process
- Occurrences of data subject complaints to the Regulator (ICO)
- Number of privacy assessments (DPIAs) against new projects
- Personal information held outside of retention period in systems.

Learning and service design improvements will be fed back to service areas as required.

13 Related Policies & Procedures

The key related policies, procedures and guidance are;

- IT Security and Usage Policy
- IT Usage Guidance
- Information Security Event (Data Breach) Procedure
- Supporting Individual Data Subject Rights Procedure
- Ad-Hoc Information Requests Procedure
- Customer Verification Procedure
- Permission to Share Procedure
- Data Sharing Guidance
- Safe Data Transfer Guidance
- Surveillance Procedure
- DPIA Template
- AI Risk Assessment template
- Marketing Guidance
- Good Information Management Guide

- Document Catalogue & Retention Schedule
- AsterNet Data Protection Guidance page

Governance			
Effective from:	26/02/2024	**Expires:**	25/02/2027
Policy Owner:	Governance & Risk Director		
Policy Author:	Head of Risk & Compliance (Data Protection Officer)		
Approved by:	*Operational Strategy Assurance Panel*		
Delegation Matrix Reference:	RO27	**Version Number:**	v8.01

Glossary

Data Subject - the identified or identifiable living individual to whom personal data relates.

Processing - an operation or set of operations which is performed on personal data, or on sets of personal data, such as:

- collection, recording, organisation, structuring or storage;
- adaptation or alteration;
- retrieval, consultation or use;
- disclosure by transmission, dissemination or otherwise making available;
- alignment or combination; or
- restriction, erasure or destruction.

Data Controller – an organisation that determines the purposes for which and the manner in which any personal data is, or is to be, processed.

Data Processor – an organisation who processes the data on behalf of the data controller.

Information Commissioners Office (ICO) - is the supervisory body for data protection in the UK. It has a number of investigative and corrective powers, as enshrined in the Act.