Data Protection, Privacy and Confidentiality Policy

ASTER GROUP

1 Scope

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

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

1.3 Aster Group is the data controller of the information that it collects and manages. 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.

This policy applies to all personal data processed by Aster.

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

1.5 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 is committed to protecting the rights and privacy of individuals.

2.2 Data Protection principles are derived from the UK General Data Protection Regulations and Data Protection Act 2018, jointly referred to in this policy as 'the Act'. We demonstrate compliance with these principles by ensuring that personal data is:

- **processed lawfully, fairly and in a transparent manner** in relation to individuals;
- **collected for specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with the original purposes;
- **adequate, relevant and limited to what is necessary** for the purpose;
- **accurate and kept up to date**; every reasonable step is taken to ensure personal data is accurate, having regard to the purposes for which it is processed, and is erased or rectified without delay;
- kept in a form which **identifies data subjects for no longer than is necessary**; and
- processed with **appropriate security** using technical and organisational measures.

3 Processing 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;

	Including but not limited to;
Name, address and 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 and date of birth, gender
National identifiers	National Insurance or social security 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

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

- **consent,** which should only be used when a genuine choice can be offered
- for the **performance of a contract** or to take steps to enter into a contract
- for compliance with a **legal obligation** (including a court order)
- to protect the **vital interests** of an individual or another person (i.e. life or death)
- for the performance of a task carried out in the **public interest**
- in the **legitimate interests** of Aster or a third party, except where such interests are overridden by the interests, rights or freedoms of the individual

3.3 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.

3.4 Special categories of personal data or 'sensitive data' include;

- 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**

3.5 We recognise that special category data needs more protection and will 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).

3.6 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.

3.7 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, requiring a positive action to say yes
- separate from other terms and conditions

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

3.9 We are committed to inclusivity and fairness, where diversity in all its forms is celebrated. When we encourage our colleagues and customers to be open about who they are, we will ensure that any wider communication of this information or their story only happens with their knowledge and support – their consent.

3.10 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

4 Sharing Data

4.1 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.

4.2 Examples of appropriate data sharing include;

Permission	The individual has given permission for Aster to share information with others. This may include family, friends or elected representatives as examples.
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
Data processing under instruction from Aster	Providing information to a third party data processor so they can perform a service for us i.e. a mailing house or IT platform
Protection of Asters financial interests	Such as ensuring utility companies direct utility charges to those responsible for paying them.

4.3 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.

4.4 We will always share data safely and securely using appropriate technical protection measures.

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

5 Data Retention, Minimisation and Cleansing

5.1 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 usually 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.

5.2 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 or historical schedules of works.

5.3 Our Information Management and Retention Procedure provides guidance to colleagues on Asters approach to disposal or retention of all information and data and includes our retention schedule.

6 Data Subject Rights

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

Individual rights	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.

6.2 Our Individual Data Subject Right Procedure provides guidance to colleagues.

7 Information Security Events - Data Breaches

7.1 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

7.2 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.

7.3 All breaches or suspected breaches will be investigated in accordance with this procedure. As required by the Act, 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.

7.4 If a breach is likely to result in a high risk to the rights and freedoms of individuals, 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.

8 Accountability

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. We will maintain a DPIA register.

8.3 Our DPIA Template supports colleagues to consider data protection and deliver the maximum possible privacy by design.

8.4 We are committed to ensuring the security of information held in our IT systems. 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.

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

- A self-learn module to be completed by all office-based colleagues within 3 months of joining and repeated annually.
- Non office-based colleagues will receive training via alternative means, tailored to their role.
- Role specific training will be delivered such as enhanced customer verification training to contact centre colleagues.
- Regular awareness initiatives will support the formal learning.
- Technical data protection specialists will have access to the training required to ensure their knowledge remains up to date.

9 Roles and Responsibilities

9.1 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.

9.2 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

9.3 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.

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

9.5 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 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.

9.6 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 & Compliance Committee.

9.7 Leaders in each service area are responsible for;

- Understanding what information is held, changes made through addition or deletion, information flows and who has access and why.
- Understanding and addressing the risks to that information and ensuring it is used in ways that are compatible with the Act.

9.8 The Information Governance team provide data protection advice and support.

9.9 Under the Transformation Network, the DP Influencers consider data protection issues in general and provide support to the Data Protection Officer in the implementation of good data protection practices in their business area.

9.10 All colleagues are responsible for complying with data protection policy, procedure and guidance.

10 Related Policies and Procedures

10.1 The key related policies, procedures and guidance are;

- IT Security and Usage Policy
- AsterNet Data Protection Guidance page
- Good Information Management Guide
- Data Sharing Guidance
- Safe Data Transfer Guidance
- Surveillance Procedure
- DPIA Template
- Marketing Guidance
- Supporting Individual Data Subject Rights Procedure
- Ad-Hoc Requests Procedure
- Information Security Event (Data Breach) Procedure
- Customer Verification Procedure
- IT Guidance

11 Governance			
Effective From:	01/02/2021	**Expires:**	31/01/2024
Policy Owner:	Governance & Risk Director		
Policy Author:	Data Protection Officer (Head of Risk & Compliance)		
Approved by:	*Group Risk & Compliance Committee*		
Delegation Matrix Reference:	R027	**Version Number:**	V7.0

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.