Consumer Information Security Policy

Issued: December 10th, 2020

APPLIES TO: All Consumers and AST – Entire Organization

PURPOSE: AST needs to gather and use certain information about individuals. These individuals can include customers, suppliers, business contacts, employees and other people the organization has a relationship with or may need to contact. This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards — and to comply with the law.

POLICY:

WHY THIS POLICY EXISTS

This data protection policy ensures AST:

- Complies with data protection laws and follows exceptional data practices
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

DATA PROTECTION LAW

The Data Protection Act 1998 describes how organizations — including AST — must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles that are foundational elements of other data protection laws, including GDPR and CCPA. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

PEOPLE, RISKS AND RESPONSIBILITIES

This policy applies to:

- The head office of AST
- All branches of AST
- All staff and volunteers of AST
- All contractors, suppliers and other people working on behalf of AST

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of current data privacy laws, as AST takes a proactive stance on protecting personal information. This data can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Device IDs
- Social Media Account IDs
- Any other information relating to individuals

DATA PROTECTION RISKS

This policy helps to protect AST and consumers from very real data security risks, including:

- Breaches of confidentiality, e.g. information being given out inappropriately.
- Failing to offer choice, e.g. all individuals should be free to choose how the company uses data relating to them.
- Reputational damage, e.g. the company could suffer if hackers successfully gained access to sensitive data.

RESPONSIBILITIES

Everyone who works for or with AST has responsibility for ensuring data is collected, stored and handled appropriately. Each team that handles personal data must ensure that it is handled and processed in line with this policy, AST's internal Information Security Policy and AST's otherwise stated data protection principles. However, these people have key areas of responsibility:

- The executive team, led by Justin Winter/CEO, is ultimately responsible for ensuring that AST meets its legal obligations.
- The executive team is responsible for:
    - Keeping apprised of data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging data protection training and advice for the people covered by this policy.
    - Handling data protection questions from staff and anyone else covered by this policy.
    - Dealing with requests from individuals to see the data AST holds about them (also called 'subject access requests').
    - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - Performing regular checks and scans to ensure security hardware and software is functioning properly.
    - Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.
    - Approving any data protection statements attached to communications such as emails and letters.
    - Addressing any data protection queries from journalists or media outlets like newspapers.
    - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

GENERAL AST STAFF GUIDELINES

- The only people able to access data covered by this policy should be those who need it to fulfil their work-related responsibilities.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- AST will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorized people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their manager or the data protection officer if they are unsure about any aspect of data protection.

DATA STORAGE

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to dataprivacy@astcorporation.com.

When data is stored on paper, it should be kept in a secure place where unauthorized people cannot access or view it. These guidelines also apply to data that is usually stored electronically but has been printed out.

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorized people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.
- When data is stored electronically, it must be protected from unauthorized access, accidental deletion and malicious hacking attempts:
- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a CD, DVD or a USB Flash Drive), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to approved cloud computing services.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.

- Data should never be saved directly to laptops or other mobile devices like tablets or smartphones.
- All servers and computers containing data should be protected by approved security software and a firewall.

DATA USE

Personal data is of no value to AST unless the business can make use of it for a valid business purpose. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft.

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorized external contacts.
- Personal data should never be transferred outside of the European Economic Area if it originates from the EEA.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

DATA ACCURACY

The law requires AST to take reasonable steps to ensure data is kept accurate and up to date. The more important it is that the personal data is accurate, the greater the effort AST should put into ensuring its accuracy. It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- AST will make it easy for data subjects to update the information AST holds about them. For instance, via the company website.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
- It is the marketing manager's responsibility to ensure marketing databases are checked against industry suppression files every six months.

SUBJECT ACCESS REQUESTS

All individuals who are the subject of personal data held by AST are entitled to:

- Know what information the company holds about them and why.
- Know how to gain access to it.
- Know how to keep personal data up to date.
- Know how the company is meeting its data protection obligations.
- Request that personal information be deleted (with some exceptions).
- Opt out of the sale of their personal information.
- Non-discrimination for exercising their data rights.

If an individual contacts the company requesting this information, this is called a subject access request. Subject access requests from individuals should be made by email, addressed to the data controller at dataprivacy@astcorporation.com. The data controller will aim to provide the relevant data within 5 business days. The data controller will always verify the identity of anyone making a subject access request before handing over any information.

DISCLOSING DATA FOR OTHER REASONS

In certain circumstances, the Data Protection Act, GDPR, CCPA and other legal policies allow personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, AST will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

PROVIDING INFORMATION

AST aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights
- That they will never be penalized for exercising their rights

To these ends, the company has a consumer data privacy notice, setting out how data relating to individuals is used by the company. This is available on request. A version of this statement is also available on the AST website.

Revision History

Version	Date of Revision	Author	Description of Changes
1.0	December 10, 2020	AST	Initial version
1.1	February 2022	AST	Annual Review