**Data Protection Policy**

**Introduction**

Airport Angels Student Services Ltd (AASSL) needs to gather, use and keep certain information. These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with.

This policy describes how this personal data must be collected, handled and stored to comply with the Data Protection Principles, which are set out in the Data Protection Act 1998 / GDPR.

**Why this policy exists**

This data protection policy ensures AASSL:

* Complies with data protection law
* 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

**Status of the Policy**

This policy does not form part of the contractual contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by AASSL. Any failures to follow the policy can therefore result in disciplinary proceedings.

**Data Protection Law**

The Data Protection Act 1998 / GDPR describe how organisations – including AASSL – must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

In summary these state that personal data shall:

* Be obtained and processed fairly and lawfully.
* Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
* Be adequate, relevant and not excessive for those purposes.
* Be accurate and kept up to date
* Not to be held for any longer than necessary
* Processed in accordance with the rights of data subjects
* Be kept safe from unauthorised access
* Not to be transferred outside the European Economic Area, unless that country or territory also ensures an adequate level of protection.

**Responsibilities**

Everyone who works for, or with, AASSL has some responsibility for ensuring data is collected, stored and handled appropriately. Each staff member that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

* The **Board of Directors** is ultimately responsible for ensuring that AASSL meets its legal obligations.
* The **Data Protection Officer** is responsible for:
* Keeping the board updated about data protection responsibilities, risks and issues.
* Reviewing all data protection procedures and related policies, in line with an agreed schedule.
* Arranging all 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 AASSL holds about them.
* Checking and approving any contracts or agreements with third parties that may handle the company’s sensitive data.
* The **IT Manager** is responsible for:
* 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.

**Responsibilities of Staff**

All staff are responsible for:

* Checking that any information that they provide to AASSL in connection with their employment is accurate and up to date.
* Informing AASSL of any changesto information, which they have provided, e.g. Changes of address.
* Informing AASS of any errors or changes in staff information. AASSL cannot be held responsible for any such errors unless the staff member has informed AASSL of them.
* When, as part of their responsibilities, staff hold information about other people they must comply with the *Guidelines for Staff* (Appendix 1)

**Subject Access Requests (SAR’s)**

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

* Ask what information the company holds about them and why.
* Ask how to gain access to it
* Be informed how to keep it up to date
* Be informed how the company is meeting its data protection obligations.

If an individual contacts the company requesting this information, this is called a subject access request. 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 allows personal data to be disclosed to law enforcement agencies without the consent of data subject.

Under these circumstances AASSL 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 advisors where necessary.

**Providing Information**

AASSL 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

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

**Compliance**

Compliance with the act is the responsibility of all members of AASSL. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to AASSL facilities being withdrawn, or even a criminal prosecution. It also may result in personal liability for the individual. Any questions or concerns about the interpretation or operation of this policy should be taken up with the Data Protection Officer.

**Guidelines for Staff – Appendix 1**

1. Members of staff will process personal data on a regular basis. AASSL will ensure that staff and customers give their consent to processing and are notified of the categories of processing, as required by the Act.
2. Information about an individual’s

* physical or mental health
* sexual life; political or religious views
* trade union membership
* ethnicity or race;
* the commission of criminal offences and court proceedings dealing with criminal offences

is sensitive and can normally only be collected and processed with the persons express consent.

1. Members of staff have a duty to make sure that they comply with the data protection principles, which are set out in the AASSL Data Protection Policy. In particular, staff must ensure that records are :

* Accurate
* Up-to-date
* Fair
* Kept and disposed of safely, and in accordance with AASSL policy.

1. Individual members of staff are responsible for ensuring that all data they are holding is kept securely.
2. Members of staff must not disclose personal data, unless for administrative or pastoral purposes, without authorisation or agreement from the Data Protection Officer, or line manager.

**Staff Checklist**

* Do you really need to record the information?
* Is the information ‘standard’ or ‘sensitive’?
* If it is sensitive, do you have the data subject’s express consent?
* Has the individual been told that this type of data will be processed?
* Are you authorised to collect/store/process the data?
* If yes, have you checked with the data subject that the data is accurate?
* Are you sure the data is secure?
* If you do not have the data subject’s consent to process, are you satisfied that one of the other conditions for processing the data applies?
* How long do you need to keep the data for, what is the rules/procedure for destruction?

**Glossary of Terms**

**Data**

Any information held by AASSL for the purpose of the business

**Personal Data**

Information about a living person. This information is protected by the Act.

**Data Subject**

The person about whom the data is held.

**Sensitive Data**

The Act introduces categories of sensitive personal data, namely, personal data consisting of information as to:

* The racial or ethnic origin of the data subject
* Their political beliefs
* Their religious beliefs or other beliefs of a similar nature
* Whether they are the member of a trade union
* Their physical or mental health or condition
* Their sexual life
* The commission or alleged commission by them of any offence or
* Any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

**Data Controller**

A person (or organisation) who determines the purposes for which, and the manner in which, any personal data are, or are to be, processed.

**Processing**

Covers almost anything which is done with or to the data including:

* Obtaining data
* Recording or entering data onto the files
* Holding data, or keeping it on file without doing anything with it or to it.
* Organising, altering or adapting data in any way
* Retrieving, consulting or otherwise using the data
* Disclosing data either by giving it out, by sending it on email, or simply making it available
* Combining data with other information
* Destroying and erasing data