Injectable Aesthetics Academy Ltd
Data Protection Policy

Injectable Aesthetics Academy Ltd

Data Protection Policy

Version 1.2

Date 06/10/2021

Author: Assad Latif

Intended Audience: All Staff, Learners and Partners.

Data Protection Policy Statement

Injectable Aesthetics Academy Ltd is registered as a data controller with the Information Commissioner's Office and the Company's' Data Protection Officer is the Records and Information Compliance Manager Assad Khan Latif.

The Company undertakes to process personal information within the terms of the Data Protection Act 1998. In accordance with the Act, the Company's must provide the Information Commissioner with details of the processing of personal data carried out by the Company's through its formal registration

The Company undertakes to maintain data in secure conditions and to process and disclose data only within the terms of its Data Protection notification.

Data Protection Policy Statement for Students

The Company processes data relating to its students for the following purposes:
maintenance of the student record and management of academic processes

- the management of Company social events
- the provision by the Company of advice and support to students
- internal research into improving education and educational services and quality and performance monitoring
- statutory requirements under the Further & Higher Education Act 1992, under the auspices of the Funding Councils

Student information is disclosed to a variety of third parties or their agents, notably:

1. relevant government departments to whom we have a statutory obligation to release information (including the SFA (Skills Funding Agency & ESF)

2. Government departments on matters relating to the prevention and detection of crime, apprehension and prosecution of offenders and/or the collection of tax (Disclosures to include but not limited to; HMRC, UK Border Agency, Police)
3. current or potential employers of our students with the individual's consent
4. current or potential providers of education to our students. This covers & Partner Colleges.
5. CPD (Continual Professional Development) and relevant insurance underwriters

NB. Disclosures to organisations not listed above will be made in specific legitimate circumstances. Consent from the student will be sought where necessary and students will be informed of such disclosures unless exceptional circumstances apply.

Data Protection Policy Statement - Staff data

The Company's processes data relating to its staff for the following purposes:

- Staff administration (including recruitment, appointment, to make payments, pension provision and for the management of sickness absence)

- To provide access and use of Company's facilities and services (including library services, sports facilities)
- To enable the Company to meet its business and legal obligations (including audit functions, marketing and promotion of the institution, health and safety, course administration)
- The Company's will, where necessary, disclose personal information relating to Company's employees to external organisations including:

➢ Government departments on matters relating to the prevention and detection of crime, apprehension and prosecution of offenders and/or the collection of tax (Disclosures to include but not limited to; HMRC, UK Border Agency, Police)

➢ Potential employers or providers of education

NB. Disclosures to organisations not listed above will be made in specific legitimate circumstances. Consent will be sought where necessary and employees will be informed of such disclosures unless exceptional circumstances apply.

Under the Data Protection Act 1998, you have a right to request and receive a copy of the current personal information held on you by the Company and a right to object to data processing that is inaccurate or, causes substantial unwarranted damage or substantial unwarranted distress. On request the Company's will also inform you of the credit agencies it has contacted and the personal details it has disclosed to them.

Please e-mail: assad@innovatelearning.co.uk if you have any specific questions relating to the Data Protection Policy, or for details of procedures relating to your rights as a data subject.

Please note that we are reliant on you for much of the data we hold: help us keep your record up-to-date by notifying your Learning Centre or the Human Resource Department of any alterations to your address, personal details, or course enrolments.

Obligations Placed Upon the Company by the Data Protection Act

The Data Protection Act 1998 is a piece of information rights legislation that covers personal information.

It aims to ensure personal privacy, through giving individuals rights with regards to information about themselves and putting responsibilities on organisations who process this information.

The Act places certain obligations with which the Company, as Data Controller, must comply:

To notify the Information Commissioner annually of the purposes for which it processes personal data

To allow individuals to find out what information is held about them, the purposes for which the information is kept, where we obtain it from and to whom we might disclose it

To process personal information in accordance with the Eight Principles of Data Processing as set out in the legislation

To Notify the Information Commissioner

Under the Data Protection Act 1998, the Company's is required to notify the Information Commissioner of the purposes for which it processes personal data. This notification is renewed annually and recorded in the Data Protection Public Register.

The Company's must ensure that its notification remains up-to-date and personal data must not be processed unless the activity is covered by the current notification.

The Rights of Individuals

Data Subjects have a number of rights relating to the information held on them as well as what happens to that data:

Right to subject access

The Data Protection Act gives Data Subjects the right to request for, in writing, a copy of information held relating to the individual in electronic format and also in some manual filing systems.

In addition individuals are also entitled to be given a description of the information, what you use it for, who you might pass it on to, and any information you have about the source of the information. This information is provided to individuals at their time of entry into the Company and is available on the Information Governance web pages.

Right to prevent processing likely to cause damage or distress

A data subject is entitled to write to the Company's to prevent processing for a specified purpose if that processing of their personal data is likely to cause unwarranted substantial damage or substantial distress to themselves or another person.

Damage can cover financial loss, loss such as pain and suffering, loss of amenity, and loss of reputation. Distress can cover shock, fear, anxiety or grief.

This right cannot be exercised if the data subject consented to the processing, the processing is part of a contract with the data subject, the processing is necessary to protect the vital interests of the data subject, or the Company's is under a legal obligation to process that data.

Right to prevent processing for the purposes of direct marketing

An individual is entitled by written notice, to require the Company's to cease, or not to begin, processing personal data for the purpose of direct marketing. When the Company's as Data Controller receives such a notice, they must comply as soon as they can. There are no exceptions to this.

The data subject may apply to Court for an order if the data controller fails to comply with the notice.

Direct marketing is defined in the Act for the purposes of this provision as meaning the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals.

Rights in relation to automated decision taking

A data subject has the right to require the Company not to make a decision that significantly affects them if it is based solely on the processing of data by automatic means.

The examples of this type of activity are assessing credit-worthiness, performance at work or possible employment, and automated assessment for academic work of students. All data subjects will be informed in advance as to whether such processing of their personal data will be undertaken.

Right to take action for compensation if the individual suffers damage by any contravention of the Act by the data controller

Data owners should be aware that a data subject now has the right to compensation either for damage or damage and distress for any contravention of the Act by the Company's. If the contravention was in relation to artistic or literary purposes or journalism, then compensation can be for distress alone.

A defence allowed in the Act is that the Company's has taken 'such care as is in all the circumstances was reasonably required to comply with the requirement concerned' Data owners should therefore ensure that, where the risk to data subjects is clearly foreseeable, appropriate measures should be taken to comply with the Act in those circumstances.

Right to take action to rectify, block, erase or destroy inaccurate data

An individual may apply to the Court for an order that would require the Company to rectify, block, erase or destroy data relating to that individual that are inaccurate together with any other personal data relating to the data subject which contain an expression of opinion which the Court finds is based on the inaccurate data. Data is considered as being inaccurate if they are incorrect or misleading as to any matter of fact.

Data owners within the Company need to ensure that there are procedures in place for data subjects to correct inaccurate or out of date data, and procedures for staff and students to update basic terms of data.

How to Complain

The Company's aims to comply fully with its obligations under the Data Protection Act 1998 and takes complaints relating to the institutions adherence to the Act very seriously.

Stage 1

Individuals wishing to report concerns relating to the Data Protection Act 1998, should, in the first instance, contact the Company's Information Compliance Officer who will aim to resolve any issues.

Mr Ahmed Usman
5 Berhem Mews
Blythe Road
West Kensington
London
WV14 0HN

email:ahmed@injectableaestheticsacade

my.com

Stage 2

If the individual feels the complaint has not been dealt with to their satisfaction, the individual can formally complain to the Records and Information Compliance Manager.

The Records and Information Compliance Manager will review the facts of the complaint and having taken this into consideration will determine whether the Company's has acted in accordance with/ or contrary to the Act.

Mr. Assad Latif
Records and Information Compliance Manager

The Records and Information Compliance Manager will contact the individual making the complaint and advise them of the outcome of the investigation into their complaint.

Stage 3

If at any time the complainant is unhappy with the way their grievance is being handled, the complainant can also contact the Information Commissioner's Office, who regulates the processing of personal information who is responsible for the regulating the processing of personal information. The ICO can be contacted:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF
Tel: 08456 306060 or 01625 545745 e-mail: mail@ico.gsi.gov.uk

Processing Personal Information in Accordance with the Eight Data Protection Principles

To comply with the Act, the Company's must ensure that it processes data in accordance with the Data Protection Principles:

Principle 1 - Personal data shall be processed fairly and lawfully.

All Personal Data processed must satisfy at least one of the conditions of Schedule 2 of the Act. The requirements of Schedule 2 can be summarised as follows:

The Data subject has consented to the processing.

To perform a contract to which the data subject is a party or to take steps at the request of the data subject so that such a contract can be entered.

To comply with a legal obligation imposed on the data controller otherwise than by a contract.
To protect the vital interests of the data subject.

For the administration of justice.

For the exercise of any function conferred by an enactment.

For the exercise of any functions of the Crown, a Minister of the Crown or a government department.

For the exercise of any function of a public nature exercised in the public interest.

For the data Controller or any third party to whom the Data is disclosed to pursue their legitimate interests.

Other specific circumstances that may be ordered by the Secretary of State from time to time.

There are special provisions within the Act for processing of sensitive personal data. Within the context of the data protection, sensitive personal data relates to the following:

- The racial or ethnic origin of the data subject
- Their political opinions
- Their religious beliefs or other beliefs of a similar nature
- Their membership of a trade union
- Their physical or mental health or condition
- Their sexual life
- The commission or alleged commission by the individual of any offence
- Any proceedings for any offence committed or alleged to have been committed by the individual, the disposal of such proceedings or the sentence of any court in such proceedings.
- When handling sensitive personal information, the data controller must ensure that in addition to complying with one of the conditions of the Schedule 2 conditions listed above, they must also comply with one of the following conditions:
- Explicit consent has been received from the data subject;
- Processing is required to comply with employment legislation;

- Processing is necessary to safeguard the vital interests of the data subject or another person; The information has already been made public by the data subject;
- Processing is necessary in connection with legal proceedings;
- Processing is necessary for the administration of justice;
- Processing is necessary for medical reasons;
- Processing is necessary for ethnic monitoring.

The Company will, during its work regularly process personal information relating to both staff and students that is sensitive in its nature. Within the context of the Company's, Departments such as Finance could process information relating to staff membership of the trade bodies.

Principle 2 - Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes. The use of modern information systems with integrated databases enables more sharing of data and reduces the need for multiple collection points for that data. Consequently, data owners should exercise great care in ensuring that data processed for one purpose is not processed for a different purpose in breach of this Principle.

Principle 3 - Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Data owners should ensure that only relevant data is processed. Neither the Company nor its staff can collect personal information on the premise that it might be useful at some stage in the future. If there is no reason to collect the data for a specified purpose, then it should not be collected.

Principle 4 - Personal data shall be accurate and, where necessary, kept up to date.

It is essential that checks for accuracy are made for maintenance of the Company data. Data owners should put in place procedures for ensuring that the data is verified for accuracy and the data is kept up to date. A basic minimum would be annual updating for both staff and student data, together with rapid updating for specific items of data.

Principle 5 - Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

Personal data should not be kept for longer than is required for the purpose for which it has been acquired. The Company's has policies and procedures in place which cover the retention of personal data relating to data subjects and further guidance can be obtained from the Company's Records Manager.

Principle 6 - Personal data shall be processed in accordance with the rights of data subjects. The Data Protection Act 1998 gives the data subject increased rights of access to personal data held on them. The Act also provides strict time limits in which data controllers must respond to access requests from individuals.

Subject to some exceptions, requests for personal information must be dealt with within 40 days of the access request being received in the Company's

Principle 7 - Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

The Company as Data Controller must ensure the security and safekeeping of all personal data whether it is held on computer or within manual files. This includes physical security from unauthorised access as well as protection against accidental loss, destruction or damage.

Principle 8 - Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The European Economic Area (EEA) consists of the 15 European member states together with Iceland, Liechtenstein and Norway. Transfers for any other states will not be legal unless their local laws provided data subjects with the same or greater levels of protection as the Data Protection Act.

In order to transfer personal information to a country outside of the EEA, Company's staff should contact the Information Compliance Officer to receive further clarification.

Privacy and Electronic Communications Regulations 2003

The Privacy and Electronic Communications Regulations 2003 regulate direct marketing activities by electronic means (by telephone, fax, email/other electronic methods) and the security and confidentiality of these communications, together with rules governing the use of 'cookies' and 'spyware"

All direct marketing undertaken by the Company's must be undertaken in compliance with the Privacy and Electronic Communications Regulations 2003.

Cookies

The Company's website collects certain personal information through the use of Cookies. Further information on the type of data collected and the Company's policy on Cookies is available on the Company's Website Privacy Policy pages.