
Data Protection Policy - GDPR

Rationale

Our Website is committed to a policy of protecting the rights and privacy of individuals, including learners, staff and others, in accordance with the General Data Protection Regulation (GDPR) May 2018.

The new regulatory environment demands higher transparency and accountability in how website manage and use personal data. It also accords new and stronger rights for individuals to understand and control that use.

The GDPR contains provisions that the website will need to be aware of as data controllers, including provisions intended to enhance the protection of client's personal data. For example, the GDPR requires that:

We must ensure that our website privacy notices are written in a clear, plain way that the clients will understand.

Our Website needs to process certain information about its clients with whom it has a relationship for various purposes such as, but not limited to:

1. The registration & Login process of the client.
2. The administration & Support services that the website provide.
3. Trading environment.
4. Phone recording progress.
5. Payment process that usually done by third parties (The PSP company).
6. Complying with legal obligations to funding bodies and government including local government.

To comply with various legal obligations, including the obligations imposed on it by the General Data Protection Regulation (GDPR) Our Website must ensure that all this information about individuals is collected and used fairly, stored safely and securely, and not disclosed to any third party unlawfully.

Compliance

This policy applies to all the website clients. Any breach of this policy or of the Regulation itself will be considered an offence and the website's disciplinary procedures will be invoked.

As a matter of best practice, other agencies and individuals working with the website and who have access to personal information, will be expected to read and comply with this policy. It is expected that departments who are responsible for dealing with external bodies will take the responsibility for ensuring that such bodies sign a

contract which among other things will include an agreement to abide by this policy.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments to the GDPR and other relevant legislation.

The Code of Practice on GDPR for the website gives further detailed guidance and website undertakes to adopt and comply with this Code of Practice.

General Data Protection Regulation (GDPR)

This piece of legislation comes in to force on the 25th May 2018. The GDPR regulates the processing of personal data, and protects the rights and privacy of all living individuals (including children), for example by giving all individuals who are the subject of personal data a general right of access to the personal data which relates to them. Individuals can exercise the right to gain access to their information by means of a 'subject access request' (by the website support). Personal data is information relating to an individual and may be in hard or soft copy (paper/manual files; electronic records; photographs; Client KYC; CCTV images etc.), and may include facts or opinions about a person.

Responsibilities under the GDPR

Our website will be the 'data controller' under the terms of the legislation.

This means it is ultimately responsible for controlling the use and processing of the personal data. Our website appoints a Data Protection Officer (The Website support manager) currently the Principal who is available to address any concerns regarding the data held by Website and how it is processed, held and used. Our website also has a nominated governor who oversees this policy.

The Senior Leadership Team is responsible for all day-to-day data protection matters, and will be responsible for ensuring that all members of staff and relevant individuals abide by this policy, and for developing and encouraging good information handling within the website.

The Senior Leadership Team is also responsible for ensuring that the website's notification is kept accurate. Details of the website's notification can be found on the Office of the Information Commissioner's website.

Compliance with the legislation is the responsibility of all website who process personal information and the third parties that using that information.

Individuals who provide personal data to the website are responsible for ensuring that the information is accurate and up-to-date, and giving the approval to use those personal data.

Data Protection Principles

The legislation places a responsibility on every data controller to process any personal data in accordance with the eight principles.

In order to comply with its obligations and undertakes to adhere to the eight principles:

1) Process personal data fairly and lawfully.

Our website will make all reasonable efforts to ensure that individuals who are the focus of the personal data (data subjects) are informed of the identity of the data controller, the purposes of the processing, any disclosures to third parties that are envisaged; given an indication of the period for which the data will be kept, and any other information which may be relevant. For example,

2) Process the data for the specific and lawful purpose for which it collected that data and not further process the data in a manner incompatible with this purpose.

Our website will ensure that the reason for which it collected the data originally is the only reason for which it processes those data, unless the individual is informed of any additional processing before it takes place. (Usually done by third party)

3) Ensure that the data is adequate, relevant and not excessive in relation to the purpose for which it is processed.

Our website will not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this mind. If any irrelevant data are given by individuals, they will be destroyed immediately.

4) Keep personal data accurate and, where necessary, up to date.

Our website will review and update all data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that this is accurate, and each individual should notify the website if, for example, a change in circumstances mean that the data needs to be updated. It is the responsibility of the website to ensure that any notification regarding the change is noted and acted on.

5) Only keep personal data for as long as is necessary.

Our website undertakes not to retain personal data for longer than is necessary to ensure compliance with the legislation, and any other statutory requirements. This means the website will undertake a regular review of the information held and implement a weeding process.

Our website will dispose of any personal data in a way that protects the rights and privacy of the individual concerned (e.g. secure electronic deletion, shredding and disposal of hard copy files as confidential waste). A log will be kept of the records destroyed.

6) Process personal data in accordance with the rights of the data subject under the legislation.

Individuals have various rights under the legislation including a right to:

- be told the nature of the information the website holds and any parties to whom this may be disclosed.
- prevent processing likely to cause damage or distress.
- prevent processing for purposes of direct marketing.
- be informed about the mechanics of any automated decision taking process that will significantly affect them.
- not have significant decisions that will affect them taken solely by automated process.
- take action to rectify, block, erase or destroy inaccurate data.
- request that the Office of the Information Commissioner assess whether any provision of the Act has been contravened.

Our website will only process personal data in accordance with individuals' rights.

7) Put appropriate technical and organisational measures in place against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of data.

Our website will do the best in order to ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorized third parties.

Our website will ensure that all personal data is accessible only to those who have a valid reason for using it.

Our website will have in place appropriate security measures e.g. ensuring that hard copy personal data is kept in lockable filing cabinets/cupboards with controlled access (with the keys then held securely in a key cabinet with controlled access):

- keeping all personal data in a lockable cabinet with key-controlled access.
- password protecting personal data held electronically.
- archiving personal data which are then kept securely (lockable cabinet).
- placing any PCs or terminals, CCTV camera screens etc. that show personal data so that they are not visible except to authorised staff.

- ensuring that PC screens are not left unattended without a password protected screen-saver being used.

In addition, our website will put in place appropriate measures for the deletion of personal data - manual records will be shredded or disposed of as 'confidential waste' and appropriate contract terms will be put in place with any third parties undertaking this work. Hard drives of redundant PCs will be wiped clean before disposal or if that is not possible, destroyed physically. A log will be kept of the records destroyed.

This policy also applies to any party who process personal data 'off-site', e.g. when working at home, and in circumstances additional care must be taken regarding the security of the data.

8) Ensure that no personal data is transferred to a country or a territory outside the European Economic Area (EEA) unless that country or territory ensures adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Our website will not transfer data to such territories without the explicit consent of the individual.

This also applies to publishing information on the Internet - because transfer of data can include placing data on a website that can be accessed from outside the EEA - so our website will always seek the consent of individuals before placing any personal data (including photographs) on its website.

While our website collecting personal data in any form via its website, and the website provide a clear and detailed privacy statement prominently on the website, and wherever else personal data is collected.

Consent as a basis for processing

Although it is not always necessary to gain consent from individuals before processing their data, it is often the best way to ensure that data is collected and processed in an open and transparent manner.

Consent is especially important when website is processing any sensitive data, as defined by the legislation.

Our website understands consent to mean that the individual has been fully informed of the intended processing and has signified their agreement (e.g. via the enrolment form) whilst being of a sound mind and without having any undue influence exerted upon them.

Consent obtained on the basis of misleading information will not be a valid basis for processing. Consent cannot be inferred from the non-response to a communication.

"Personal Details

- *For the purposes of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679 you consent to the website holding and*

processing personal data including sensitive personal data of which you are the subject, details of which are specified in the website data protection policy.

- *This will include marketing images and the client KYC.*

Our website will ensure that any forms used to gather data on an individual will contain a statement (fair collection statement) explaining the use of that data, how the data may be disclosed and also indicate whether or not the individual needs to consent to the processing.

How We Use Your Personal Information

Your information may be shared with third parties (Including Processors), this will only take place where the law allows it and the sharing is in compliance with the Data Protection Act 1998.

You can opt out of contact for other purposes

By post.

By phone.

By email.

By request to support department .

Our website will ensure that if the individual does not give his/her consent for the processing, and there is no other lawful basis on which to process the data, then steps will be taken to ensure that processing of that data does not take place.

Subject Access Rights (SARs)

Individuals have a right to access any personal data relating to them which are held by the website. Any individual wishing to exercise this right should apply in writing to the website support team.

Under the terms of the legislation, any such requests must be complied with within 40 days.

Disclosure of Data

Our website undertakes not to disclose personal data to unauthorised third parties, including family members, friends, government bodies and in some circumstances, the police.

Legitimate disclosures may occur in the following instances:

- the individual has given their consent to the disclosure.
- its a legitimate interests of the website.
- the disclosure is required for the performance of a contract.

There are other instances when the legislation permits disclosure without the consent of the individual.

Publication of Website Information

Our website publishes various items which will include some personal data, e.g.

- internal telephone directory.
- Client KYC Documents.
- photos and information in marketing materials.

It may be that in some circumstances an individual wishes their data processed for such reasons to be kept confidential, or restricted our website access only. Therefore it is website policy to offer an opportunity to opt-out of the publication of such when collecting the information.

Email

It is the policy of our website to ensure that senders and recipients of email are made aware that under the DPA, and Freedom of Information Legislation, the contents of email may have to be disclosed in response to a request for information. One means by which this will be communicated will be by a disclaimer on our support team email.

Under the Regulation of Investigatory Powers Act 2000, Lawful Business Practice Regulations, any email sent to or from our website may be accessed by someone other than the recipient for system management and security purposes.

cookies

We make use of following types of cookies:

- Strictly necessary cookies. These cookies are required for the operation of our website. They include, for example, cookies that enable you to log into secure areas of our website, save images into a light box, use a shopping cart, and access account information.
- Functionality cookies. These are used to recognize you when you return to our website. This enables us to personalize our content for you, greet you by name, remember your preferences (for example, your choice of language or country), and to allow you to have a interactive chat with a support representative.
- Analytical/performance/testing cookies. They allow us to recognize and count the number of visitors and to see how visitors move around our website when they are using it. This helps us to improve the way our website works, for example, by ensuring that users are finding what they are looking for easily. These allow us to provide you with a consistent experience as we test different versions of features and functionality.

You may block cookies by activating the setting on your browser that allows you to refuse the setting of all or some cookies. However, if you use your browser settings to block all cookies (including essential cookies) you may not be able to access all or parts of our site."

Procedure for review

This policy will be updated as necessary to reflect best practice or future amendments made to the General Data Protection Regulation (GDPR) May 2018 and Data Protection Act 1998.

For help or advice on any data protection or freedom of information issues, please do not hesitate to contact:

The Data Protection Officer (DPO) by using our support team email address.
