# GDPR Policy

**Introduction**

The General Data Protection Regulations (GDPR) came into force on 25th May 2018. The Data Protection Act 1998 (DPA) will be superseded by a new DPA that enacts the GDPR's requirements. For the purposes of this policy, as the case may be, we are data controller as well as data processor under the GDPR.

**General Code of Practice – For Data Controller**

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and where necessary, kept up to date.
- Processed in a manner that ensures appropriate security of the data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organizational measures.

**General Code of Practice – For Data Processor**

- The processor must only act on the written instructions of the controller (unless required by law to act without such instructions).
- The processor must ensure that people processing the data are subject to a duty of confidence.
- The processor must take appropriate measures to ensure the security of processing.
- The processor must only engage a sub-processor with the prior consent of the data controller.
- The processor must assist the data controller in providing subject access and allowing data subjects to exercise their rights under the GDPR.
- The processor must assist the data controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments.
- The processor must delete or return all personal data to the controller as requested at the end of the contract.
- The processor must submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

**What we collect**

We may collect, process, store and use the following information:

- Personal Identification information (Name, email, Phone number)
- Gender
- Date of birth
- National Insurance Number
- Ethnicity
- Home Address and Postcode
- Learning Difficulty and Health Problems
- Prior qualifications
- Employment status
- IP address from where they register
- Email Marketing preferences
- System & Browser details

The data is collected by us when you visit website learnflo.co.uk to enrol for our services, enter into agreement with us and/or third party, request us to provide information about yourself to third party government agencies and accreditation bodies for funding purposes, assessments, communicate with us over telephone or in any other matter such as web chat, SMS, fax or email. Kindly note

that in addition to collecting data directly from you, we may also obtain data about you from our carefully chosen training providers and other third-party service providers. However, failure by you to provide personal data when requested by us may mean that we are unable to provide certain services and products to you.

**How do we collect data**

We collect and process data when customers:

- Register online or place an order for any of our Programs or courses.
- Posts an enquiry from any of our landing pages or web sites.
- Use or view our website via your browser's cookies.
- Responds to our marketing campaigns and social media advertisements

We may also receive customer data indirectly from the following sources:

- Partners programs
- Resellers

Customer data is collected from sites secured with 256-bit SSL encryption.

**How we use data**

Will use customer data for various purposes including but not limited to:

- Enrol learners for training programs
- Develop individual learning plans for training programs
- Asses learning
- Carry out your requests, fulfill orders
- Communicate with you about your orders, account with us, including any requests, questions or comments you may have.
- We may send data to, and also use the resulting information from, government agencies and accreditation bodies
- Service administration related to the service, activity or online content you have signed up for including notifying you that a particular service, activity or online content has been suspended for maintenance, etc.
- Provide customer support, including processing any concerns about our services.
- Using IP addresses and device identifiers to identify the location of users, blocking disruptive use, establishing the number of visits from different countries, tailoring the content of our sites, apps or other services based on browsing behaviours, and determining which country you are accessing the services from.
- Enrol customers on e-Careers Apprenticeships or third-party Learning Management System on the registered programs.
- May request customers later to provide their feedback on the orders processed and, on the courses learning.
- Send notifications to remind of Live class schedule, date and time
- Send notifications to make sure they stick with their learning plan and timelines, making sure they achieve their goals within the allocated time.

**How do we store and protect data**

- All our customers data are stored securely on Microsoft Azure with the datacenter located in UK (South) (Using LearnFlo, our Learning Management System)
- Customers credentials are encrypted using a complex algorithm before storing them in a database.

- We carefully review the all the forms collecting data to make sure we are collecting only the relevant and required data to process their order and enrol them on a course.
- Customers data are stored securely in a SQL database hosted on Microsoft Azure and the credentials are encrypted with a complex algorithm before storing.
- We review the access logs periodically to make sure the right number of users have access to the right amount of data.

**How long the data is stored**

We will keep your personal information for as long as we need it for the purpose it is being processed for.

We also make sure the data held with us is accurate and up to date to provide best possible customer service.

If you sign up for our newsletters / marketing communications, we will keep your personal information until such time you request that your information is deleted by you electing to unsubscribing which can be done at any time. We will still retain some of your personal information in order to ensure that you are not contacted again.

Your personal information may also be retained so that we can continue to improve your experience with us.

**Legal rights for the customers**

As per GDPR, following legal rights are available for each customer:

- The right to be informed - You have the right to be provided with clear, concise, transparent, intelligible and easily understandable information about how we use your personal data and your rights. This information is provided in this Privacy Policy.

- The right to access - You have the right to access your personal information which we hold. You can receive a copy of the personal information we hold about you by contacting us at dpo@e-careers.com. Kindly note that, your right to access your personal information is not absolute as there may be instances where applicable law or regulatory requirements allow or require us to refuse to provide some or all of the personal information we hold about you.

- The right to rectification - You have the right to have your inaccurate personal data we hold about you to be rectified or completed if it is incomplete. We understand the importance of this data accuracy and should you want to exercise your rights, then contact us at dpo@e-careers.com. In certain circumstances, we might refuse a request for rectification especially if we believe that the personal information, we hold about you is accurate.

- The right to erasure - You have the right to have your personal data erased and this right to erasure is also known as the 'the right to be forgotten'. You can request us to delete your data and we will take reasonable steps to respond to your request in accordance with the legal requirements. Kindly note that, your right of erasure is not absolute, and we can only comply with your request for erasure, if the personal data we collect is no longer needed for any purposes and we are not required by law to retain it.

- The right to restrict processing - You have the right to request restrictions or suppression of your personal data. Kindly note that, the right to restrict processing is not an absolute right and only applies in certain circumstances. When you restrict the processing of your data, we will store your personal data, but we will not use it.

- The right to data portability - You have the right to data portability, which will allow you to obtain and reuse your personal information we hold about you for your own purposes across different services. We will provide to you, or a third party you have chosen, your information in a structured commonly used, machine readable format.

Kindly note that, this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.

- The right to object - You have the right to object to us for processing your information under certain types of processing, including processing for direct marketing. In some cases, we may demonstrate that we have compelling reasons to process your information or have legal obligations in doing so.

- Rights in relation to automated decision making and profiling - You have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal or significant effects on you. You have the right to obtain human intervention, express your point of view, obtain an explanation of the decision reached after assessment and challenge such decision. This right does not apply if the automated decision is a contractual necessity between us and you, if its authorized by law and / or based on your explicit consent.

**Who has access to customer data**

- Onboarding team to carry out enrolment processes across the relevant government agencies
- Training support team to resolve any issues related to their course access and delivery.
- Technical support team to resolve any issues related to the course content or access to the systems.
- Internal quality assurance team to ensure that Training team deliver quality learning in line with regulatory requirements
- Second Line support team at LearnFlo who have access for the purposes of resolving complex technical issues and retrieving data for the purposes of Data Subject Access Requests where our technical team are unable to carry out such requests independently.
- Each team have been provided with the right level of access to customer data. Every activity e-Careers Apprenticeship team performs on customers account is logged with the date and timestamp and it is reviewed periodically to make any changes to improve security.

**Monitoring and review**

- We will monitor the effectiveness of this policy and will review the implementation of it on a regular basis to assess its suitability, adequacy, and effectiveness.
- Internal control systems and procedures which are designed to prevent any breach of GDPR regulations are subject to regular audits to ensure that they are effective in practice. Hence, any identified improvements will be applied as soon as possible.

- **Name: Tolu Fagbola**
- **ICO Security Number - CSN6302642**

- **Position: Director of Apprenticeships and Data Protection Officer**

- **Signature:** 

- **Date: 4th February 2022**