WimX Learning (Wimbledon Experience Ltd)

Data Protection and Records Retention Policy (Review Date: 07.9.24)

Introduction

WimX Learning takes its responsibilities with regard to the management of the requirements of the General Data Protection Regulation (GDPR) very seriously. This policy sets out how WimX Learning manages those responsibilities.

WimX Learning obtains, uses, stores and otherwise processes personal data relating to potential staff and learners (applicants), current staff and learners, former staff and learners, current and former workers, contractors, website users and contacts, collectively referred to in this policy as data subjects. When processing personal data, WimX Learning is obliged to fulfil individuals' reasonable expectations of privacy by complying with GDPR and other relevant data protection legislation (data protection law).

This policy therefore seeks to ensure that we:

1. are clear about how personal data must be processed and WimX Learning's expectations for all those who process personal data on its behalf;
2. comply with the data protection law and with good practice;
3. protect WimX Learning's reputation by ensuring the personal data entrusted to us is processed in accordance with data subjects' rights
4. protect the WimX Learning from risks of personal data breaches and other breaches of data protection law.

Scope

This policy applies to all personal data we process regardless of the location where that personal data is stored (e.g. on a personnel's own device) and regardless of the data subject. All staff and others processing personal data on WimX Learning's behalf must read it. A failure to comply with this policy may result in disciplinary action.

This data protection and records retention policy is to ensure compliance with the Data Protection Act 2018 and General Data Protection Regulation (GDPR).

As a responsible awarding organisation, WimX Learning aims to robustly implement the requirements of the GDPR. Part of meeting the the obligations of GDPR is the production and implementation of this policy.

WimX Learning is fully committed to protecting the rights and privacy of individuals operating in accordance with the statutory legislation outlined within the GDPR. In doing so we are committed to protecting the privacy and confidentiality of data provided to us. Any decisions for the disclosure, retention or disposal of information are made in line with relevant legislation.

Information about our personnel, learners and other individuals will only be used in line with established regulations. Personal data will be collected, recorded and used fairly, stored safely and securely and not disclosed to any third party unlawfully. This also includes sensitive information such as ethnic background, political opinions, religious beliefs, health, sexual health and criminal records.

It is ultimately the responsibility of the Head of the Centre, Victoria Davies, to ensure that this policy is published, accessible and implemented across all personnel, learners and by any relevant third parties. However, the Qualification Coordinators (QCs) specific to each qualification are responsible for ensuring this information is fully understood by their qualification team and also by the learners who commence courses/programmes in their area.

Objectives

As the lawful and correct treatment of personal data is critical to our successful operations and to maintaining confidence, WimX Learning is committed to operate in line with GDPR. Please see WimX IT Policy.

Data Breach Procedure

Steps to take:

1. Seek to secure a further breach of system

2. If breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms we will inform those individuals without due delay

3. Provide information and advice to the individuals to help them protect themselves from its effects

4. Inform any related Controllers without due delay (If a Controllers is involved they would inform the individuals unless they wish us to do so)

5. Inform ICO within 72 hours of becoming aware of the breach 6. Keep a record of the breach