GDPR DATA PROTECTION/RETENTION POLICY STATEMENT

Introduction

The reputation of the **School of Marketing** and future growth depends on how we manage and protect Personal Data. Protecting the confidentiality and integrity of Personal Data is a key responsibility of everyone within the organisation. As an organisation that collects, uses and stores Personal Data about its employees, suppliers, learners, and employers, the **School of Marketing** recognises that having controls around the collection, use, retention and destruction of Personal Data is important in order to comply with the obligations under Data Protection Laws and in particular its obligations under Article 5 of **GDPR**.

All members of staff are obliged to comply with this Policy at all times.

If you have any queries concerning this Policy, please contact the **Data Protection Officer**, who is responsible for ensuring the organisation's compliance with this Policy.

The **School of Marketing** has implemented this **Data Protection Policy** to ensure all staff are aware of what they must do to ensure the correct and lawful treatment of Personal Data. This will maintain confidence in the organisation and will provide for a successful working and learning environment for all.

All staff will receive a copy of this Policy when they start and will have access to the policy through the staff intranet.

The policy will be reviewed annually and periodically when revisions are required.

2. About this policy

This Policy sets out the basis on which the **School of Marketing** will collect and use Personal Data either where the **School of Marketing** collects it from individuals itself, or where it is provided to the organisation by third parties. It also sets out rules on how we handle, use, transfer and store Personal Data.

It applies to all Personal Data stored electronically, in paper form, or otherwise.

3. Definitions

3.1 The **School of Marketing** - the organisation and all its sites.

3.2 Employee - any employee who accesses any of the organisation's Personal Data and will include: employees, consultants and temporary personnel hired to work on behalf of the organisation.

3.3 Controller – Any entity (e.g. company, organisation or person) that makes its own decisions about

how it is going to collect and use Personal Data. A Controller is responsible for compliance with Data Protection Laws. The **School of Marketing** will be viewed as a Controller of Personal Data if it decides what Personal Data it is going to collect and how it will use it. It is the organisation itself which is the Controller and not individuals.

3.4 Data Protection Laws – The **General Data Protection Regulation (Regulation (EU) 2016/679)** and all applicable laws relating to the collection and use of Personal Data and privacy and any applicable codes of practice issued by a regulator including in the UK, the **Data Protection Act 2018**.

3.5 Data Protection Officer – Our **Data Protection Officer** is **David Porter (Director of Product)** and can be contacted at: **david@schoolofmarketing.co.uk**

3.6 ICO – the **Information Commissioner's Office** which is the UK's data protection regulator

3.7 Individuals – living individuals who can be identified, *directly or indirectly*, from information that the **School of Marketing** has. For example, an individual could be identified directly by name, or indirectly by gender, job role and office location if you can use this information to work out who they are. Individuals include employees, learners, partner agencies, employers, contractors, visitors and potential learners.

3.8 Personal Data – any information about an Individual which identifies them or allows them to be identified in conjunction with other information that is held. It includes information of this type, even if used in a business context. Personal data is defined broadly and covers things such as name, address, email address (including in a business context, email addresses of Individuals in companies such as firstname.surname@organisation.com), IP address and also more sensitive types of data such as trade union membership, genetic data and religious beliefs. These more sensitive types of data are called "Special Categories of Personal Data". Special Categories of Personal Data are given extra protection by Data Protection Laws.

3.9 Processor – any entity (e.g. company, organisation or person) which accesses or uses Personal Data on the instruction of a Controller. A Processor is a third party that processes Personal Data on behalf of the Controller. This is usually as a result of the outsourcing of a service by the Controller or the provision of services by the Processor which involve access to or use of Personal Data. Examples include: where software support for a system, which contains Personal Data, is provided by someone outside the business; cloud arrangements; and mail fulfilment services.

3.10 Special Categories of Personal Data – Personal Data that reveals a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data (i.e. information about their inherited or acquired genetic characteristics), biometric data (i.e. information about their physical, physiological or behavioural characteristics such as facial images and fingerprints), physical or mental health, sexual life or sexual orientation and criminal record. Special Categories of Personal Data are subject to additional controls in comparison to ordinary Personal Data.

4. The School of Marketing General Obligations

4.1 All employees must comply with this policy.

4.2 All employees must ensure that they keep confidential all Personal Data that they collect, store, use and come into contact with during the performance of their duties.

4.3 Employees must not release or disclose any Personal Data outside the organisation and inside the organisation not authorised to access the Personal Data, without specific authorisation from the Finance Director, their manager or the **Data Protection Officer**. This includes by phone calls or email.

4.4 Employees must take all steps to ensure there is no unauthorised access to Personal Data whether by other employees who are not authorised to see such Personal Data or by people outside the organisation

5. Data Protection Principles

It is necessary for the **School of Marketing** to collect and process data on our learners and staff. The **School of Marketing** will strive to observe the law in all aspects of handling data and will only use data for legitimate purposes.

The **School of Marketing** will also strive to maintain the following due care in processing data. The **School of Marketing** will ensure data is timely, accurate, secure and confidential.

All staff at the **School of Marketing** are made aware that handling personal data is a sensitive issue and will not disclose data without the consent of the data subject or as a legal or operational requirement. Where data is disclosed to other agencies a contract exists for the transfer of this data and transactions always take place in good faith.

The **School of Marketing** subscribes to the eight principles of good practice:

1. Data is fairly and lawfully processed
2. Data is processed for limited purposes
3. Data is adequate, relevant and not excessive
4. Data is accurate
5. Data is not kept longer than necessary
6. Data is processed in accordance with data subject's rights
7. Data is secure
8. Data is not transferred to countries without adequate protection

6. Lawful Use of Personal Data

6.1 In order to collect and/or use Personal Data lawfully the **School of Marketing** needs to be able to show that its use meets one of a number of legal grounds.

6.2 In addition when the **School of Marketing** collects and/or uses Special Categories of Personal Data, the **School of Marketing** has to show that one of a number of additional conditions is met

6.3 The **School of Marketing** has assessed how it uses Personal Data and how it complies with the obligations set out in paragraphs **6.1** and **6.2**. If the **School of Marketing** changes how it uses Personal Data, the organisation needs to update this record and may also need to notify Individuals about the change. If the **School of Marketing** therefore intends to change how we use Personal Data at any point they must notify the **Data Protection Officer** who will decide whether their intended use requires amendments to be made and any other controls which need to apply.

- Data is fairly and lawfully processed

*The **School of Marketing** needs to collect certain information about our students and staff. We collect only information we need to and we are registered with the **Data Commissioner** to keep this information. We process this information for business needs and this is done fairly and without prejudice using software and manual systems we are licensed to use. We will not share our information with other agencies unless we are licensed to do this or we have specifically requested permission from the data subject.*

- Data is processed for limited purposes

*We only collect the minimum amount of information that is required. We then only use this information for the purpose it was collected for. We are registered with the **Data Commissioner** to process certain information for specific purposes.*

- Data is adequate, relevant and not excessive

We only collect the minimum amount of information that is required. This information is required to allow us to support our staff and customers.

- Data is accurate

We try to ensure that data is kept accurate and where data subjects information changes we update our information as soon as we can. We will make changes to the data as soon as we are notified it is inaccurate.

- Data is not kept longer than necessary

We are obliged by legislation to keep information collected for certain timescales. Where possible we archive older data where it is accessible but secure. Once data is deemed to be no longer required it is destroyed by a method appropriate to how it is held, this is done securely and confidentially.

- Data is processed in accordance with data subject's rights

Data is maintained confidentiality and all work carried out on or with the data is bound by the basic principles of this policy.

- Data is secure

Data is kept in secure areas and access to data is limited to those who need to use it as a requirement of their work. Electronic data is held securely with password access. Paper based information is filed in a secure manner and wherever practicable in locked rooms and/or cupboards.

- Data is not transferred to countries without adequate protection

Data is kept in secure areas and access to data is limited to those who need to use it as a requirement of their work. Electronic data is held securely with password access. Paper based information is filed in a secure manner and wherever practicable in locked rooms and/or cupboards.

7. Privacy Notices

7.1 Where the **School of Marketing** collects Personal Data directly from Individuals, the organisation will inform them about how the **School of Marketing** uses their Personal Data. This is in a privacy notice.

7.2 If the **School of Marketing** receives Personal Data about an Individual from other sources, the **School of Marketing** will provide the Individual with a privacy notice about how the **School of Marketing** will use their Personal Data. This will be provided as soon as reasonably possible and in any event within one month. Apprenticeship Commitment and Learning Plan seeks consent about the information that is stored and will be used and how contact is made with the learner.

7.3 If the **School of Marketing** changes how it uses Personal Data, the organisation may need to notify Individuals about the change. If a **School of Marketing** employee therefore intends to change how they use Personal Data please notify the **Data Protection Officer** who will decide whether the intended use requires amendments to be made to the privacy notices and any other controls which need to apply.

8. Data Quality – ensuring the use of accurate, up to date and relevant personal data

8.1 Data Protection Laws require that the **School of Marketing** only collects and processes Personal Data to the extent that it is required for the specific purpose(s) notified to the Individual in a privacy notice. The **School of Marketing** is also required to ensure that the Personal Data held is accurate and kept up to date.

8.2 All employees that collect and record Personal Data shall ensure that the Personal Data is recorded accurately, is kept up to date and shall also ensure that they limit the collection and recording of Personal Data to that which is adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used.

8.3 All employees that obtain Personal Data from sources outside the organisation shall take reasonable steps to ensure that the Personal Data is recorded accurately, is up to date and limited to that which is adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used. This does not require employees to independently check the Personal Data obtained.

8.4 In order to maintain the quality of Personal Data, all employees that access Personal Data shall ensure that they review, maintain and update it to ensure that it remains accurate, up to date, adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used. Please note that this does not apply to Personal Data which the **School of Marketing** must keep in its original form (e.g. for legal reasons or that which is relevant to an investigation).

8.5 The **School of Marketing** recognises the importance of ensuring that Personal Data is amended, rectified, erased or its use restricted where this is appropriate under Data Protection Laws. Any

request from an individual for the amendment, rectification, erasure or restriction of the use of their Personal Data should be referred to the **Data Protection Officer**.

9. Retention

9.1 Data Protection Laws require that the **School of Marketing** does not keep Personal Data longer than is necessary for the purpose or purposes for which the **School of Marketing** collected it.

9.2 The **School of Marketing** has assessed the types of Personal Data that it holds and the purposes it uses it for and has set retention periods for the different types of Personal Data processed by the **School of Marketing**, the reasons for those retention periods and how the organisation securely deletes Personal Data at the end of those periods.

9.3 If employees feel that a particular item of Personal Data needs to be kept for more or less time than the retention period, for example because there is a requirement of law, or if an employee has any questions about this Policy or Personal Data retention practices, they should contact the **Data Protection Officer** for guidance.

10. Data Security

10.1 The **School of Marketing** takes information security very seriously and has measures against unlawful or unauthorised processing of Personal Data and against accidental loss of, or damage to, Personal Data. The organisation has in place procedures and technologies to maintain the security of all Personal Data.

11. Data Breach

11.1 Whilst the **School of Marketing** takes information security seriously, it is possible that a security breach could happen which may result in the unauthorised loss of, access to, deletion of, or alteration of Personal Data. If this happens there will be a Personal Data breach and employees must comply with the **School of Marketing** Data Breach Notification process and complete **Appendix 1**.

Please familiarise yourself with it as it contains important obligations which employees need to comply with in the event of Personal Data breaches.

11.2 Personal Data breach is defined as any failure to keep Personal Data secure, which leads to the accidental or unlawful loss (including loss of access to), destruction, alteration or unauthorised disclosure of Personal Data. Whilst most Personal Data breaches happen as a result of action taken by a third party, they can also occur as a result of something someone internal does.

11.3 There are three main types of Personal Data breach which are as follows:

11.3.1 Confidentiality breach - where there is unauthorised or accidental disclosure of, or access to, Personal Data e.g. hacking, accessing internal systems that an employee is not authorised to access, accessing Personal Data stored on a lost laptop, phone or other device, people "blagging" access to Personal Data they have no right to access, putting the wrong letter in the wrong envelope, sending an email to the wrong learner, or disclosing information over the phone to the wrong person.

11.3.2 Availability breach - where there is an accidental or unauthorised loss of access to, or

destruction of, Personal Data e.g. loss of a memory stick, laptop or device, infection of systems by ransomware, deleting Personal Data in error, loss of access to Personal Data stored on systems or inability to restore access to Personal Data from backup.

11.3.3 Integrity breach - where there is an unauthorised or accidental alteration of Personal Data.

Breaches of data which could be damaging to the business:

I. **Public Data breach -** information intended for public use or information that can be made public without any negative impact.
II. **Internal Data breach -** information regarding the day to day operation of the business which is primarily for staff use but may be useful for a 3rd party.
III. **Confidential Data breach -** information about the business (capital/financial/intellectual) that people within the business only need to know as part of their job role.
IV. **Highly Confidential data breach -** information that will cause significant damage to the business and reputation or would lead to a breach of the **Data Protection Act**.

12. What you should do in the event of a security breach

12.1 Report immediately to the **Finance Director** and **Data Protection Officer.**

12.2 Complete **Appendix 1** and send it to the **Finance Director** and **Data Protection Officer** within 24 hours.

13. Individuals' rights

13.1. Subject Access Requests

13.1.1 Individuals have the right under the **GDPR** to ask the **School of Marketing** to confirm what Personal Data they hold in relation to them and provide them with the data. This is not a new right but additional information has to be provided and the timescale for providing it has been reduced from 40 days to one month (with a possible extension if it is a complex request). In addition, you will no longer be able to charge a fee for complying with the request.

13.1.2 Subject Access Requests are becoming more and more common and are often made in the context of a dispute which means that it is crucial that they are handled appropriately to avoid a complaint being made to the ICO.

13.2 Right of Erasure (Right to be Forgotten)

13.2.1 This is a limited right for individuals to request the erasure of Personal Data concerning them where:

13.2.2 The use of the Personal Data is no longer necessary.

13.2.3 Their consent is withdrawn and there is no other legal ground for the processing.

13.2.4 The individual objects to the processing and there are no overriding legitimate grounds for the processing.

13.2.5 The Personal Data has been unlawfully processed.

13.2.6 The Personal Data has to be erased for compliance with a legal obligation.

13.2.7 In a marketing context, where Personal Data is collected and processed for direct marketing purposes, the individual has a right to object to processing at any time. Where the individual objects, the Personal Data must not be processed for such purposes.

13.3 Right of Data Portability

13.3.1 An individual has the right to request that data concerning them is provided to them in a structured, commonly used and machine-readable format where:

13.3.2 The processing is based on consent or on a contract; and

13.3.3 The processing is carried out by automated means

13.3.4 This right isn't the same as subject access and is intended to give individuals a subset of their data.

13.4 The Right of Rectification and Restriction

13.4.1 Individuals are also given the right to request that any Personal Data is rectified if inaccurate and to have use of their Personal Data restricted to particular purposes in certain circumstances.

13.4.2 The **School of Marketing** will use all Personal Data in accordance with the rights given to Individuals' under Data Protection Laws and will ensure that it allows Individuals to exercise their rights in accordance with the data protection principles.

14. Data Protection Impact Assessments (DPIA)

14.1 The **GDPR** introduced a new requirement to carry out a risk assessment in relation to the use of Personal Data for a new service, product or process. This must be done prior to the processing via a **Data Protection Impact Assessment (DPIA)**. A **DPIA** should be started early in the design of processing operations. A **DPIA** is an assessment of issues affecting Personal Data which need to be considered before a new product/service/process is rolled out. The process is designed to:

14.1.1 Describe the collection and use of Personal Data.

14.1.2 Assess its necessity and its proportionality in relation to the purposes 14.1.3. Assess the risks to the rights and freedoms of individuals.

14.1.4 Assess the measures to address the risks.

15. Transferring personal data to a country outside the EEA

15.1 Data Protection Laws impose strict controls on Personal Data being transferred outside the **EEA.** Transfer includes sending Personal Data outside the **EEA** but also includes storage of Personal Data or access to it outside the **EEA**.

15.2 So that the **School of Marketing** can ensure it is compliant with **Data Protection Laws**, employees must not export Personal Data unless it has been approved by the **Data Protection Officer**.

16. Your Rights

Access

You have a right to request to view any information held by any organisation about you. All learners and/or employees have the right to view their data files whether electronically held or paper based. In the first instance you contact the **Finance Director** or **Data Protection Officer**. A **School of Marketing** representative will write back confirming receipt of the form and detailing when and where you can view the data in accordance with the timeframes set out. This in no way affects your rights.

Confidentiality

Personal Data is kept as confidentially as possible and all records are kept secure. The nature of all conversations is considered confidential unless there is a legal need for another party to know the information. If you feel that your confidentially has been breached, then you should contact the **Finance Director** or **Data Protection Officer** to investigate the matter.

Appeals

You have the right to appeal about how your data is being used. This appeal should in the first instance be raised via the Complaints procedure.

Appendix 1: Data Incident Report Form

Description of the data breach	
Time & date data breach was identified and by whom	
Name and role of person reporting the data breach	
Contact details	

Classification of breach (Personal Data/Business Sensitive)	
Volume of data involved	
Breach contained or on-going	
If on- going what actions are being taken to recover the data?	
Who has been informed?	
Other relevant information	
Evaluation of severity of incident- major/serious/minor	
Response/actions/decision required -by whom and by when	

Who needs to be notified?	
By whom and by when?	