Title: **Data Protection and Retention Policy** Ref: PY07 Version: 2

1. Introduction, Scope & Purpose

1.1. This Confidentiality and Data Retention Policy covers all information and data generated, held, controlled, created or otherwise used by MetaGedu Apprenticeships.

2. Policy Overview

2.1. Reasons for this policy

This policy provides a framework for ensuring that MetaGedu Apprenticeships meets its obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 18). It is to ensure all information held about its learners, staff and customers are held securely and confidentially in accordance with the legal requirements and best practice.

2.2. Data Protection

MetaGedu Apprenticeships is registered with the Information Commissioner's Office (ICO) and can be found on the register. We take data protection very seriously and as such complies with the principles set out in the UK GDPR

Data Protection Principles

MetaGedu complies with data protection legislation guided by the six data protection principles.

In summary, they require that personal data is:

- processed fairly, lawfully and in a transparent manner.
- used only for limited, specified stated purposes and not used or disclosed in any way incompatible with those purposes.
- adequate, relevant, and limited to what is necessary.
- accurate and, where necessary, up to date.
- not kept for longer than necessary; and
- kept safe and secure**.**

In addition, the accountability principle requires us to be able to evidence our compliance with the above six principles and make sure that we do not put individuals at risk because of processing their personal data. Failure to do so can result in a breach of legislation, reputational damage, or financial implications due to fines. To meet our obligations, we put in place appropriate and effective measures to make sure we comply with data protection law.

2.3. Personal Data

The UK GDPR definition of "personal data" includes any information relating to an identified or identifiable natural living person. Pseudonymised personal data is covered by the legislation, however
anonymised data is not regulated by the UK GDPR or DPA 18, providing the anonymisation has not been done in a reversible way.

Some personal data is more sensitive and is afforded more protection, this is information related to:

- Race or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;

- Biometric ID data;
- Health data;
- Sexual life and/or sexual orientation; and
- Criminal data (convictions and offences)

2.4. Staff, Customer and Learner Data

MetaGedu Apprenticeships holds personal data about students, parents, staff and other individuals in order to carry out its business and provide its services. For example, this information could include name, address, email address and date of birth. No matter how the data is collected, recorded and used, this personal information must be dealt with properly to ensure compliance with data protection legislation. Access to all personal information is restricted to only those who have a legitimate requirement to use or view the information. This information is held securely with appropriate safeguards to prevent unauthorised use or access. Data held on electronic media has security protocols built into the system, such as individual access codes, which are password protected. Hard copies are retained in suitable secure storage mediums with restricted access.

2.5. Learner's evidence and assessments

Confidential information gathered directly or indirectly in the workplace will be shared only with authorised personnel. No confidential work products are permitted in learners' portfolios. Where work products contain some confidential information, the information can be removed or censored.

2.6. Control of Data

MetaGuedu will complete a Data Protection Impact Assessment (DPIA) at least annual and for any other major projects it undertake that involve processing of personal data or for any projects likely to result in a high risk to individuals. The purpose of the DPIA is to assess and minimise the risks to the individuals whos data we process. The assessment (Appendix 1) considers the likelihood and severity of any impact on individuals. If a high risk is identified that cannot be mitigated, MetaGedu must contact the Information Commisioner's Office (ICO) before starting to process any data.

2.7. Rights

MetaGedu Apprenticeships is dedicated to ensuring that the rights of individuals about whom information is held can be fully exercised under the UK GDPR. These rights are:

- The right to be informed.
- The right to access.
- The right to rectification.
- The right to erasure (the right to be forgotten).
- The right to restrict processing.
- The right to data portability.
- The right to object.
- Rights related to automated decision making including profiling.

2.8. Document Retention (Appendix 2 for full schedule)

Documents are only retained for the required amount of time relative to the regulatory authority.

Currently, this is:

- For financial/accounting reasons - 7 years from the end of the last company financial year they relate to.
- For ESFA/Funding reasons – 10 years from the funding date
- For personal data – Only for as long as required, but for at least 7 years.
- For Qualification data (assessment decisions/IQA) – 7 years from the date of certification
- Learner portfolios – until the next EQA visit
- IQA records – 3 years
- Internally marked exams for 3 years (paper-based)

2.9. Time for Policy Review

This Policy is to be reviewed annually

2.10. Dissemination

The Policy is available for current and potential clients and apprentices to view

2.11. Disclaimer

MetaGedu reserve the right to amend this Confidentiality and Data Retention policy at any time to comply with new legislation and guidance

3. Roles & Responsibilites

3.1. MetaGedu's responsibilities are to:

- Ensure that MetaGedu Apprenticeships is registered with the Information Commissioner's Office.
- Establish policies and procedures and ensure that they are up to date and comply with the law.
- Ensure that staff know about and understand this policy.
- Provide staff with data protection training.

3.2. The Compliance Officer's responsibilities are to:

- Handle subject access requests.
- Investigate data protection breaches.
- Draw up guidance on good data protection practices.
- Advise staff with data protection queries.

3.3. Staff responsibilities are to:

- Comply with this policy and any other supporting policies and procedures.
- Only access the personal data of others that they need to use.
- Make sure their own personal data provided to MetaGedu is accurate and up to date.
- Inform MetaGedu if any of their personal data changes.
- Inform MetaGedu if they become aware that any of the information that MetaGedu holds about them is not accurate.
- Ensure all personal data is kept securely.

- Ensure no personal data is disclosed either verbally or in writing to any unauthorised third party.
- Ensure personal data is kept in accordance with MetaGedu's retention schedule.
- Promptly direct any queries regarding data protection, including subject access requests, to the Compliance Officer.
- Inform the Compliance Officer of any data protection breaches as soon as possible and support the Compliance Officer in resolving breaches.

3.4. Apprentices and Other Users' responsibilities are to:

· Make sure that any personal data that they provide is accurate and up to date.
· Inform MetaGedu if any of their personal data changes.
· Inform MetaGedu if they become aware that any of the information that the College holds about them is not accurate.

4. Change History

Version	Changes made to previous version	Approved By	Date
v1	Initial release	Eric Sykes	22/02/2023
v2	Font Changes	Eric Sykes	12/06/2023

APPENDIX 1 - DATA PROTECTION IMPACT ASSESSMENT

Why is a DPIA required?

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why we have identified the need for a DPIA.

Processing

How will we be collecting, using, storing and deleting data? Will it be shared with anyone? Will the data be housed in the UK, EU or outside of the EU?

What is the scope of the processing?

What is the nature of the data, does it include special category/criminal offence data? How much data will we be using, how often who is affected and what area does it cover?

What is the context of the processing?

what is the nature of our relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are we signed up to any approved code of conduct or certification scheme (once any have been approved)?

What are the purposes for the processing?

What do we want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for us, and more broadly?

Consultation Process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Assessing necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will we prevent function creep? How will we ensure data quality and data minimisation? What information will we give individuals? How will we help to support their rights?

What measures do we take to ensure processors comply? How do we safeguard any international transfers?

Risk Identification

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, med or high

Measures to reduce Risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no

Sign off

Item	Name/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
Nominated Person advice provided:		Nominated Person should advise on compliance, step 6 measures and whether processing can proceed
Summary of Nominated Person advice:		
Nominated Person advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The Nominated Person should also review ongoing compliance with DPIA

APPENDIX 2 - RETENTION SCHEDULE DOCUMENTS INDEX

How long client records should be kept?

Assessment records	**Timescale**
Portfolios	Until External Assurance after Completion
Student assessment records – unit recording sheets, tracking documents and any other records of marks/assessment	Current year + maximum of 6 years*
Records of special arrangements, mitigating circumstances and appeals against assessment decisions	Current year + maximum of 6 years*
Minutes of Assessment Board meetings	Current year + 3 years
Assessment plans/assignment briefs	Current year, then updated
Internal Quality Assurance Records	Current + 3 years
External Quality Assurance/Examiner Reports	Current + 3 years
Teaching	
Lesson Plans/Schemes of Work	Current year, then updated
Teaching Materials/Course Handboooks	Current year, then updated
Induction programme	Current year, then updated
Quality Assurance	**Timescale**
External course submissions/validation/approval	Life of course + 4 years
Internal course validation	Current year + 1 year
Programme Quality Reviews/Quality Improvement Plans	Current year + 3 years
Student Feedback	Current year + 3 years
Minutes and notes of team meetings and activities	Current year + 3 years
Student Records	
Tutorial/Disciplinary/ILP records	Completion of student's course + 4 years
Progress reports including work experience reports	Completion of student's course + 4 years
Health and Safety	
Health & Safety including COSHH	Updated +40 years
Workshop/Work Based Risk Assessment Records	Updated +40 years
Accident Reports	Updated +40 years
Hazardous items	Decommissioning/removal + 40 years
Stocktaking	
Stocktaking records	Current + 1 year
Finance/Accounting	
Sales invoice and the processing of incoming payments	Current + 7 years
Receipts	Current + 7 years
Petty cash	Current + 7 years
Receipt and processing of apprentice fees	Current + 7 years

Funding	
For ESFA/Funding reasons	10 years from the funding date
For personal data	As long as required, but for at least 7 years
For Qualification data (assessment decisions/IQA)	7 years from the date of certification
Internally marked exams	3 years (paper-based)