UNIVERSITY ACADEMY 92

MANCHESTER

Data Protection and Information Security Policy

Implementation date:	**January 2021**
Version number:	**1.1**

Document type		Strategy
	✓	Policy
		Regulations
		Procedure
		Code of Practice
		Guidance
Area of UA92 business		Academic
		Finance
	✓	Governance & Compliance
		Marketing & Engagement
		Operations
		People
		Registry and Quality
		Student Life
		Student Recruitment and Admissions
		External Affairs
		Other
Document Name:	Data Protection and Information Security Policy	
Author:	Registrar / Digital Services Manager	
Owner (if different from above):	Registrar / Digital Services Manager	
Document control information:		
Version number:	1.1	
Date approved:	22nd January 2021	
Approved by:	UA92 Leadership Team	
Implementation date:	January 2021	
Review due:		
Document location:		
Consultation required:		
Equality & Diversity		
Legal considerations (including Consumer Rights)		
Information Governance		
Students		
Employee Engagement Forum		
External		

REVISION HISTORY			
Version	**Date**	**Revision description/Summary of changes**	**Author**
1.1	29th July 2021	Updating of areas of business and job titles.	Student Administration Assistant

		Addition of ‘apprentices’ into policy body.	

1. Purpose

1.1 The purpose of this document is to define the Data Protection Policy for University Academy 92 Limited (UA92) and to ensure UA92's compliance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

1.2 UA92 will ensure that all employees, students, apprentices, partners, volunteers, and contractors who have access to personal data held by the institution are made fully aware and trained on their responsibilities under data protection legislation.

1.3 UA92 is committed to ensuring compliance with relevant data protection laws and will:

- have in place processes to ensure that the rights of data subjects, as defined under data protection legislation, are appropriately honoured;
- implement policies and procedures to ensure that the data protection principles are adhered to when processing personal or special category information;
- ensure that it is sufficiently accountable for its information processing activities, as described within Articles 5 and 24 of the GDPR;
- ensure that records of all processing activities are maintained and regularly reviewed;
- ensure that all information processing activities have an appropriate legal basis.

1.4 Definitions

i. Personal information is data which includes information relating to a living person who can be identified or who is identifiable, directly from the data in question, or who can be indirectly identified from that information in combination with other information.

ii. Special Category information is personal information, which the GDPR states is more sensitive, and requires more protection. A full list of special category data items is available from the Information Commissioner's Office (ICO) website.

iii. The ICO is the data protection supervisory authority for the UK. The ICO has specific responsibilities set out in both the GDPR and the Data Protection Act 2018. The ICO has a range of powers where they believe organisations are not meeting their statutory requirements, ranging from criminal prosecution, the imposition of monetary penalties on organisations and the power of audit.

iv. Data Controller is the organisation that determines the purposes and means of processing of personal information.

v. Data Processor is anyone (other than an employee of the data controller) who processes data on behalf of the data controller.

vi. Anonymisation is the process of turning personal information into a form which does not identify individuals and where identification is not likely to take place. This allows for much wider use of the information.

vii. Pseudonymisation is a process where information is replaced with a pseudonym, e.g. names replaced with numbers. Pseudonymisation only provides limited protection of identity of data subjects and there is often a 'key', which will allow re-identification of individuals.

2. Scope

2.1 This Policy is applicable to all employees at UA92, including temporary, casual, volunteers, contractors and agency employees where acting on behalf of UA92.

2.2 It also applies to third party organisations who may hold information, subject to the GDPR or the Data Protection Act 2018, on behalf of UA92.

2.3 The Policy applies to students and apprentices where they are processing personal data on behalf of UA92 but not where they are processing personal data for non-UA92 or private purposes and for which UA92 is not a Data Controller.

2.4 Roles and responsibilities

2.4.1 Principal and Chief Executive Officer (CEO) has overall responsibility for the strategic and operational management of UA92 and ensuring that the institution's policies comply with all legal, statutory and good practice guidance requirements.

2.4.2 Registrar and Secretary is the Data Protection Officer (DPO) and has overall responsibility for the operation of governance at UA92 and for implementing and monitoring this Policy and any related information governance policies. They will be the first point of escalation for any issues that require senior management input and will report to the CEO where appropriate, such as where a data security breach requires consideration for reporting to the data protection regulator. They are also responsible for:

- day-to-day responsibility for monitoring compliance with this policy by all areas of UA92;
- maintaining the appropriate data protection registrations with the Information Commissioner's Office;
- ensuring that the UA92's suite of Privacy Notices are kept accurate and up-to-date;
- advising employees on any data protection issues which may arise at UA92;
- maintaining a suite of policies and standard operating procedures to ensure UA92 is compliant with appropriate data protection legislation;
- logging and investigating personal data security breaches which are reported to compliance@ua92.ac.uk.

- advising on the strategic direction of the data protection agenda at UA92;
- monitoring compliance and reviewing the success of UA92, Induction and Refresher, Information Security training and awareness raising activities.

2.4.3 The Digital Services and Innovation Manager is responsible for the day-to-day monitoring of UA92's computers, networks and data, to protect against threats such as security breaches, computer viruses, attacks by cyber criminals and credit/debit card fraud. It is the responsibility of individual systems owners to work to recommended standards, carrying out Data Protection Impact Assessments where appropriate, and to respond to concerns identified by the Digital Services and Innovation Manager. The Digital Services and Innovation Manager will be responsible for assisting the Information Governance team in investigating reported personal data security breaches.

2.4.4 All UA92 Employees including temporary, casual, volunteers and agency employees have a responsibility for compliance with this policy. All employees are responsible for being aware of the information governance requirements of UA92, including the need to maintain the confidentiality and security of personal information and the requirement to report any breaches of this policy or any applicable data protection legislation.

3. Data Protection Policy statements

3.1 Data Protection Principles

3.1.1 UA92 is required to comply with the six principles of data protection contained within Article 5 of the GDPR. These principles share similarities with the eight principles contained within the Data Protection Act 1998.

3.1.2 The six principles of GDPR are:

1. processed lawfully, fairly and in a transparent manner in relation to individuals;
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (also known as 'data minimisation');
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as

the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. Article 5(2) of the GDPR also requires that "the controller shall be responsible for, and be able to demonstrate, compliance with the principles". Non-compliance with GDPR can result in a monetary penalty notice being issued by the Information Commissioner's Office, the data protection regulatory body. Monetary penalties under GDPR can reach up to €20 million or 4% of global turnover, whichever is greater.

3.2 Lawful basis for processing

3.2.1 In order to process personal information UA92 must meet one of the legal bases contained within Article 6(1) of the GDPR.

3.2.2 In order to process special category personal information UA92 must also meet one of the legal bases contained within Article 9(2).

3.2.3 The legal basis for processing must be determined before the processing commences and are recorded within the UA92's suite of Privacy Notices.

3.2.4 For the processing of personal data to be legal under GDPR, UA92 must determine which legal basis the data is being processed under.

3.2.5 There are six legal bases listed in Article 6(1) of the GDPR:

1. **Consent:** the data subject has given clear consent for you to process their personal data for a specific purpose.
2. **Contract:** the processing is necessary for a contract you have with the data subject, or because they have asked you to take specific steps before entering into a contract.
3. **Legal Obligation:** the processing is necessary for you to comply with the law.
4. **Vital Interests:** the processing is necessary to protect someone's life.
5. **Public Task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
6. **Legitimate Interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is good reason to protect the data subject's personal data which overrides those legitimate interests.

3.3 Lawful basis for processing special category data

3.3.1 For the processing of special category data to be legal under GDPR two lawful bases of the GDPR must be met. One of the lawful bases from the six listed in Article 6(1) must be met, and one of the ten lawful bases listed in Article 9(2) must also be met.

3.3.2 The choice of legal basis under Article 6(1) does not necessarily dictate which lawful basis under Article 9(2) is most appropriate. For example, using Consent under Article 6(1) does not mean that 'Explicit Consent' under Article 9(2) must be chosen.

3.3.3 The ten lawful bases for processing special category data listed in Article 9(2) are:

1. Explicit Consent: the data subject has given explicit consent to the processing of special category data for one or more specified purposes;
2. Obligations and Rights: processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
3. Vital Interests of the data subject or another person: processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
4. Legitimate Activities: processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
5. Public Domain: processing relates to personal data which are manifestly made public by the data subject;
6. Legal Claims: processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
7. Substantial Public Interest: processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
8. Health & Social Care: processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional;

9. Public Health: processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
10. Archiving / Research: processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3.4 Privacy notices

3.4.1 In order to comply with GDPR and national data protection legislation, UA92 is required to inform data subjects of how their data will be processed. In line with the GDPR requirements, UA92 provides a Privacy Notice on its website which is:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child;
- free of charge; and
- cover UA92's processing activities.

3.5 Data minimisation

3.5.1 UA92's collection and processing of personal data will be limited to only what is necessary to achieve the purpose and aims of the processing.

3.6 Subject Access

3.6.1 Under the GDPR, any individual can make a 'subject access request' (Recital 63). Subject access requests allow data subjects to access or view their personal data and to verify the lawfulness of processing.

3.6.2 UA92 has one month to respond to these requests and a copy of the information requested must be provided free of charge in the majority of cases.

3.6.3 For further information on the right of subject access and how it is managed at UA92 please refer to the subject access request webpages or contact the Data Protection Officer.

3.7 Retention of Information

3.7.1 Data controllers are responsible for ensuring that data that they process is only kept for the period required to fulfil the purpose of why it was processed. This is enshrined in GDPR principles.

3.7.2 Individual teams at UA92 are responsible for ensuring that they comply with principles of the GDPR regarding the retention of information.

3.7.3 Guidelines on retention of information is provided via the following:

- UA92 records retention schedule;
- UA92 document retention policy.

3.8 Use of email

3.8.1 The use of email is a ubiquitous method of communication for almost all modern businesses and organisations. However, it is accepted that email is inherently unsafe for the transfer of large volumes of personal or special category data. In order to mitigate any risks associated with sending personal or special category data via email, employees are expected to follow these principles:

1. Limit the amount of personal data shared via email – only include what is absolutely necessary. E.g. “regarding the student we discussed in the meeting earlier today”, rather than “this is about XXX”
2. Consider whether initials or student number be used rather than a full name or other identifier.
3. NEVER put personal data in the ‘Subject’ line of an email. If personal data is included in the email then this should be marked as Confidential in the ‘Subject’ line.
4. High profile incidents have occurred where emails are sent to a large number of recipients and all are included into the ‘To’ or ‘CC’ field. Multiple recipients should be added into the ‘BCC’ field rather than the ‘To’ or ‘CC’ fields to limit the chances of personal data be disclosed inappropriately.
5. If required to send personal or special category data either,
    a) concerning several/many individuals or,
    b) a significant amount of information about one individual/a small group of individuals, employees should not be including this information in the body of the email. In this situation, the member of employees should drop the personal or special category data into MS Teams, share the link and password protect the attachment. The password should then be communicated to the recipient via another method, e.g. telephone call.
6. Care should be taken with forwarding email chains and including prior content in communications to other parties, to ensure that no data is unintentionally included.

4. Information Security Policy Statements

4.1 All UA92 employees are responsible for ensuring the security of information that they process as part of their role at UA92. Employees must ensure that personal information is not disclosed to any unauthorised third party. All employees must appraise themselves of the UA92’s Information Security Policy.

4.2 Storing and sharing personal /special category data in the Cloud.

4.2.1 The storing of any data or important documents on local storage, such as removable USB disks or hard drives, is not allowed. All data, where it needs

to be stored in line with this policy, should be done so in the Cloud. UA92 uses Microsoft 365..

4.2.2 UA92 has specific contracts with Microsoft (for Office 365) governing data security. UA92 data should not be stored in any other cloud storage systems. Office 365 is hosted within the EU by Microsoft and therefore there are no limits on the storage of personal or special category information. However, employees should give due consideration to applying appropriate access controls to any personal or special category information stored within Office 365.

4.2.3 It is the duty of each employee to understand the IT solutions applicable to their role and how to utilise them to ensure the principles of this policy are adhered to. Any additional training required should be discussed with the employees line manager or the Digital Services and Innovation Manager.

4.3 Information Classification

4.3.1 UA92 has four information classifications to help employees identify the level of security the information requires. The four classifications are:

Classification	Definition
Public	May be viewed by anyone, anywhere in the world
Open	Available to all members of employees
Confidential	Available only to authorised and authenticated members of employees
Highly confidential	Access is controlled and restricted to a small number of authenticated members of employees

4.3.2 Each of the four classifications has its own constraints on publication and requirements for access controls. For further information on the information classifications in use at UA92, please see the UA92 Document Retention policy.

5. Related documentation

- UA92 Document Retention policy (available on MS Teams).
- UA92 Document Retention schedule (available on MS Teams).
- UA92 Privacy statement https://www.ua92.ac.uk/privacy-policy
- IT Usage Policy.