5. Data Retention Policy[1]

(This section is to be extracted and uploaded separately on the MCAST Website Data Protection Section at https://mcast.edu.mt/data-protection-documents/)

3.1. Introduction

3.1.1. This Policy represents the policy for Malta College for Arts, Science and Technology ("MCAST", "the Data Controller", "the Organisation", "we", "our", "us") regarding the retention, archiving and disposal of physical and electronic records and documents containing personal data.

3.1.2. In the course of carrying out the various operational activities, we collect personal data relating to our students, staff, suppliers and any other individuals we interact with, from a wide range of sources and generate a substantial volume of data that are retained as physical paper and/or electronic records. Appropriate retention of data is necessary for the Organisation's operational performance and in some cases is required to fulfil statutory or other regulatory requirements and/or to evidence events.

3.1.3. Furthermore, as also outlined in its Data Protection Policy, personal data will only be retained for as long as is necessary, after which the data will be destroyed or anonymised as required. Therefore, it is vital that the Organisation establishes and maintains clear and specific policies and procedures in relation to the retention and destruction of personal data.

3.1.4. This Policy should be read alongside the Data Retention Policy which is found in Section 5 of this Policy and which provides data retention periods for various different types of personal data we hold.

3.2. Objectives

3.2.1. This Policy aims to achieve the following objectives:

a) Regulate the retention and disposal of records while adhering to the storage limitation principle to which personal data should not be retained for a longer period than necessary;
b) Promote the digitisation of documentation as may be reasonably possible in order to minimise the use of storage space, as well as to promote a sustainable use of paper and printing consumables;
c) Set out the duration of time for which records should be retained;
d) Determine the processes for disposing of records in a secure manner; and
e) Establish roles and responsibilities.

3.3. Scope

3.3.1. This Policy and the Data Retention Policy apply to all physical and electronic records and documents generated during the course of the Organisation's operations irrespective of the media on which they are created or held. This may include but is not limited to Microsoft Office suite of applications (Word, Excel, PowerPoint and Access), PDF documents, e-mails, text files, images, audio and video footage, physical memos, papers and documents, etc.

3.4. Roles and responsibilities

3.4.1. It is the responsibility of the Data Protection Officer (the "Policy Owner") to ensure that this Policy is implemented throughout the Organisation and that the Data Retention Policy is followed.

[1] Found at **https://mcast.edu.mt/data-protection-documents/**

3.4.2. The Policy Owner is also authorised to:

a) Make modifications to the Data Retention Policy outlined in Section 5 to ensure that it is in compliance with the General Data Protection Regulation (2016/679) and Union/member state laws, as may be amended from time to time;
b) Annually review the Data Retention Policy; and
c) Monitor compliance to this Policy.

3.4.3. The Policy Owner will reach out to the Authorised Employees (the "Data Set Owners") to establish their respective data retention periods and purposes, and together carry out subsequent annual reviews. The Data Set Owners are responsible for ensuring that all physical and electronic records and documents containing personal data that are within their control are retained and destroyed in accordance with this Policy and the Data Retention Policy. They must implement measures to ensure that they can identify when a retention period is due to expire, so that they can carry out a review and determine whether the personal data should be deleted or destroyed. In addition, the Data Set Owners should carry out periodic reviews at least annually of the personal data contained in the physical and electronic records and documents that are within their control (even if that personal data is not covered by a retention period contained in the Data Retention Policy), to determine whether it is being retained and destroyed in accordance with this Policy. The Data Set Owners may delegate routine tasks to others, where appropriate.

3.4.4. This policy applies to all MCAST personnel ("you" or "your") and it sets out what we expect from you to assist the Organisation to comply with its data retention and destruction obligations under data protection laws. All MCAST personnel play a vital role, and you must read and ensure that you fully understand and comply with this policy in relation to all personal data which you process on our behalf.

3.4.5. Your compliance with this policy is mandatory. Any breach of this policy may result in disciplinary action.

3.5. The Policy

3.5.1. The Organisation is required under data protection laws to ensure that physical and electronic records and documents containing personal data are not retained in a form which enables the identification of individuals for any longer than is necessary for the purposes for which the personal data have been collected. We must be able to justify our retention of personal data.

3.5.2. In practice what this means is that the Organisation must not retain the personal data contained within physical and electronic records and documents for any longer than is necessary:

a) for the operational purpose that the personal data was collected for, and which the relevant data subject has been informed of (i.e. in relevant privacy notices);
b) in order to comply with any applicable statutory or regulatory retention requirements; or
c) to enable the Organisation to exercise its legal rights and/or defend against legal claims.

3.5.3. Where a statutory or regulatory retention requirement applies, or where data is relevant to an actual or potential legal claim, only the specific personal data which is required to be retained in order to meet the statutory/regulatory retention requirement or for a legal claim, should be retained for those purposes.

3.5.4. Personal data may also be retained for a longer period if it is solely for archiving purposes in the public interest, scientific, or historical research purposes or statistical purposes, in accordance with

Article 89(1) of the GDPR. Such allowance is subject to the implementation of appropriate technical and organisational measures which are required by data protection laws, in order to safeguard the rights and freedoms of the data subject. If you believe that personal data should be retained for these purposes, please contact the Data Protection Officer by sending an email to dpo@mcast.edu.mt.

3.5.5. As a data controller, we must take a proportionate approach to data retention, balancing our needs with the impact of retention on data subjects' privacy. We also need to comply with all other aspects of data protection laws in relation to the personal data we retain, including ensuring that its retention is fair and lawful and that it is secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

3.5.6. Guideline data retention periods for different types of personal data, which should be followed by all respective Data Set Owners, are provided in the Data Retention Policy.

3.5.7. We must ensure that any request received from a data subject asking us to delete or destroy their personal data under the 'right to be forgotten' is appropriately dealt with in accordance with data protection laws. Furthermore, any such request should be dealt with in line with our Data Subjects Rights Procedures.

3.5.8. Each Data Set Owner must ensure that effective processes are in place to ensure that the personal data within their control is handled, retained, archived and deleted or destroyed in accordance with this Policy and the Data Retention Policy.

3.5.9. Prior to the expiry of the retention period for the personal data provided in the Data Retention Policy (or at regular intervals, and at least annually if no such retention period is provided), the personal data should be reviewed by the Data Set Owner, in consultation with the Policy Owner, to determine whether the Organisation should continue to retain it (or any part of it), for operational reasons, in order to comply with a statutory retention period or a regulatory obligation or for the purposes of a legal claim. If the Data Set Owner believes that the personal data needs to be retained for longer than a data retention period provided in the Data Retention Policy, they should contact the Data Protection Officer.

3.5.10. If personal data needs to be retained only for statutory or regulatory purposes or for a legal claim, the Data Set Owner should ensure that it is moved from a live environment to a secure archive that is subject to appropriate security and restricted access to ensure that the personal data is only used for that specified purpose. Once it is no longer needed for that purpose, it is the responsibility of the Data Set Owner to ensure that the personal data is securely and permanently deleted or destroyed or anonymised.

3.6. Secure Deletion/Destruction or Anonymising Data

3.6.1. Where there is no need to retain personal data any longer, it is the responsibility of the Data Set Owner to ensure that the personal data is securely and permanently deleted or destroyed in accordance with this Policy or that, as a minimum, it is anonymised. Personal data is anonymised where no data subjects can be identified from the data, either from that data alone or together with other data that the Organisation holds, has access to or may obtain access to. This also applies to any back-ups or duplicate copies of the personal data.

3.6.2. Personal data must be deleted or destroyed using one of the following secure methods:

a) Documents retained electronically should be deleted with a secure deletion utility that ensures that the information cannot be retrieved. Standard deletion utilities that only remove the file pointer should not be used.
b) Personal data on hard drives, removable media and any similar items must be securely erased before any disposal or reassignment of the equipment.
c) Where personal data cannot be erased from equipment, it must be physically destroyed by an authorised, specialist destruction company, and certificates of destruction must be obtained.
d) Paper copies must be destroyed using cross-cut shredders.

3.6.3. The Data Set Owners must approve the destruction or deletion of the personal data in advance and must record in Record Disposal Form (**MOP_ADM_001_14_REV_A_FORM_03_RECORD DISPOSAL FORM**). They must also liaise with the Data Protection Officer to ensure that the respective Records of Processing Activities are amended accordingly, if and as required.

3.7. Data Retention Periods

3.7.1. The Retention periods for the various types of data are as follows;

3.7.1.1. **Academic Data**

a) Academic Records at Registrar's Office (name, surname, identity card number, personal email address, programme and module specifications, results, academic transcripts) — 40 years form date of graduation for the purpose of issuing certificates and academic transcripts[2]

b) Admission Records (such as: Application forms and student certificates submitted and uploaded via the College's CMIS, portfolios submitted in the case of RPEL, Copies of the student identity cards, and any other documentation which is listed in the College's prospectus as a requirement for entry to a specific course) – for a period not exceeding 4 years[4]

In the case of programmes which are regulated by external bodies/authorities (such as in the case of STCW courses run at the IET – Centre for Maritime Studies), the retention periods as stipulated in the respective 3rd party regulations apply, provided tha the time frames are equal to or grater thab those of the MCAST internal standards.

c) Profile of the student population, including the prevalence of vulnerable groups, course participation, retention and success rates, students' satisfaction with their programmes, employment rates and career paths (when the course states an orientation towards employment) for a period not exceeding 4 years from date of graduation and in anonymised manner thereafter for the remaining 40 years retention period.[3]

d) Students' personal files (held at Institutes) – 4 years from the end of the student's last academic year

e) Students' personal files (held at the Registrar' Office) – Students' personal details maintained at the Registrar's office (address, mobile telephone number, home telephone and personal email address)

[2] (MFHEA National Quality Assurance Framework)

[3] (MFHEA National Quality Assurance Framework)

will be retained a period not exceeding 4 years after the student finishes their studies at MCAST, for Tracer Studies purposes only.

f) Students' sensitive data files (held at Institutes and IEU) – for a period not exceeding 3 months from when the student resigned or was dismissed from MCAST

g) Students' sensitive information (held at Students Support Services) – for a period not exceeding 5 years from when therapeutic sessions are terminated

h) Students' work held at the College/ Institute – refer to the MCAST Programme Regulations (Document numbers 003, 004 and 005[4]) for the procedure related to the Disposal of Student Work

3.7.1.2. **Administrative Data**

a) Staff personal files (including leave and sick leave records) – for a period not exceeding 10 years from when the member of staff resigned or was dismissed as per Government HR Policy

b) Staff payroll, tax and financial details – for a period not exceeding 10 years from when the member of staff resigned or was dismissed as per Government HR Policy

c) Prospective staff CVs and job application forms – for a period not exceeding 3 months from the date of the selection report for those who failed the interview and 1 year from the date of the selection report for those who were on the waiting list

d) Internal Audit Office – Files created by the internal audit office are to be retained for a period not exceeding 6 years, to allow time for IAID to perform its own audit of MCAST.

e) Grievances Office – Files created by the grievances office for a period not exceeding 5 years.

f) CCTV Footage – for a period not exceeding 7 days

g) Mailboxes and Microsoft Accounts: MCAST mailboxes and Microsoft accounts (including uploaded documentation) for Employees shall be deleted after 2 weeks from termination of employment with MCAST.

h) Mailboxes and Microsoft Accounts: MCAST mailboxes and Microsoft accounts (including uploaded documentation) for Students shall be deleted after 52 weeks from graduation from their studies at MCAST, or from deregistration or resignations.

3.8. Changes to this Policy

3.8.1. The Organisation reserves the right to change this Policy at any time. It is the data subject's obligation to refer to this Policy to identify the retention periods of its personal data.

[4] Available at: https://mcast.edu.mt/college-documents/