

Malta Business School

Data Protection Policy

Revision History			
Version Number	Revision Date	Revised by	Summary of changes
Version 0	28 th May 2014	Christine Caruana	
Version 1	7 th October 2017	Christine Caruana	Minor edits
Version 2	12 th July 2018	Christine Caruana	Updates to reflect Chapter 686 of the Data Protection Act 2018.
Version 3	7 th September 2022	Christine Caruana	Minor edits
Version 4	31 st January 2024	Christine Caruana	Inclusion of Intellectual property rights and data protection on recorded and live-streamed sessions.

Data Protection Policy

Preamble: The information and guidelines within this policy apply to the Malta Business School: the management, the staff, the educators and the learners (referred to collectively as MBS in this policy).

1. Introduction

1.1 Like other business schools, MBS holds and processes information about its employees, applicants, learners, non-resident members and other individuals for various purposes (for example, the administration of the admissions process, to enable correspondence and communication, including the provision of references and certificates).

2. Scope of Policy

2.1 This policy covers records held and processed by MBS. MBS is responsible for its own records under the terms of the 2001 National Data Protection Act, and it has submitted a separate notification to the Information and Data Protection Commissioner.

3. Summary of Aims

3.1 The lawful and correct treatment of personal information is vital for the success of the MBS operations, and to maintain confidence and trust in both MBS and the individuals with whom we deal with. Therefore, MBS will, through appropriate management, and strict application of criteria and controls:

- Fully observe conditions regarding the fair collection and use of information.
- Meet its legal obligations under the Data Protection Act to specify the purposes for why information is used.
- Collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements.
- Ensure the quality of information used.
- Apply strict checks to determine the length of time information is held.
- Ensure that the rights of people about whom information is held can be fully exercised under the Act. (These include: the right to be informed that processing is being undertaken; the right of access to one's personal information; the right to prevent processing in certain circumstances; the right to correct, rectify, block or erase information which is regarded as wrong information).
- Take appropriate technical and organisational security measures to safeguard personal information.
- Ensure that personal information is not transferred abroad without suitable safeguards.

4. Data Protection Principles

4.1 To comply with the Data Protection Act 2001 (CAP 440 of the Laws of Malta), personal data in the possession of MBS, **must** be:-

- Processed fairly and lawfully.
- Processed in accordance with good practice.
- Collected only for specific, explicitly stated, and legitimate purposes.
- Adequate and relevant in relation to the purposes of the processing.

- Correct and,
- If necessary, up to date.

4.2 To comply with the Data Protection Act 2001 (CAP 440 of the Laws of Malta), personal data in the possession of MBS, **must not** be:

- Processed for any purpose that is incompatible with that for which the information is collected.
- Other than the minimum necessary for the purposes of processing.
- Kept for a period longer than it is necessary, having regard to the purposes for which it is processed.

5. Processing

5.1 Personal data may only be processed in at least one or more of these circumstances:

- The data subject has unambiguously given his consent; or
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
- Processing is necessary for compliance with a legal obligation to which the controller is subject; or
- Processing is necessary in order to protect the vital interests of the data subject; or
- Processing is necessary for the performance of an activity that is carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data is disclosed; or
- Processing is necessary for a purpose that concerns a legitimate interest of the controller or of such a third party to whom personal data is provided, except where such interest is overridden by the interest to protect the fundamental rights and freedoms of the data subject and in particular the right to privacy.

5.2 *Non-compliance may result in disciplinary action.*

6. Notification to the Information and Data Protection Commissioner

6.1 MBS has an obligation as a Data Controller to notify the Information and Data Protection Commissioner as it is stipulated in Part VII of the Data Protection Act.

6.2 Individual data subjects can obtain full details of the data protection registration/notification process from the Commissioner's website (www.idpc.gov.mt).

7. Information and Data Protection Officer

7.1 MBS's Information and Data Protection Officer is the Head of Programmes. All queries about the data protection policy and all requests for access to personal data should be addressed to our Information and Data Protection Officer (see "Right to Access Personal Data" below).

8. Responsibilities of individual Data Users

8.1 All members of the School who record and/or process personal data in any form (called "Data Users" in this policy) must ensure that they comply with the requirements of the 2001 Act and its subsequent amendments (including the Data Protection Principles) and with the School's data protection policy (including any procedures and guidelines which may be issued from time to time). A breach of the 2001 Act and/or the School's data protection policy may result in disciplinary proceedings.

8.2 In particular, no member of the School may, without the prior written authorization of the Information and Data Protection Officer:

- Develop a new computer system for processing personal data.
- Use an existing computer system to process personal data for a new purpose.
- Create a new manual filing system containing personal data.
- Use an existing manual filing system containing personal data for a new purpose.

8.3 The above does not apply to databases which are maintained by individual Data Users within the School for their private domestic uses, for example, private address books. However, individual Data Users should consider whether their private domestic uses fall within the scope of the 2001 Act.

9. "Data Areas" and "Data Area Contacts"

9.1 To aid the efficient administration of the School's data protection policy, the data which the School holds/processes has been divided into a number of "Data Areas". These are described below, showing who may have access to the data.

9.2 In each case, there is also specified a "Data Area Contact". They will be responsible in relation to the data in the Data Area in question (and thus not simply for the files which they maintain) for the following:

- Informing the Information and Data Protection Officer of proposed processing of personal data within the School which may need to be notified to the Information and Data Protection Commissioner.
- Providing personal data to the Information and Data Protection Officer in response to a subject access request when requested to do so by the Information and Data Protection Officer, and
- Maintaining the security of, and access to, personal data within the Data Area.

9.3 The Information Data Protection Officer may from time to time designate other Data Areas and/or Data Area Contacts. The Information and Data Protection Officer or his appointee will have access to all of these data areas as required to achieve compliance with the Data Protection and Freedom of Information Acts.

10. Data Areas

10.1 Academic files

10.1.1 Academic files are maintained in respect of learners' academic progress and welfare. They may also contain financial and medical data. The purposes for which they are maintained include monitoring learners' academic progress and general welfare and administering the relevant learner's

applications for employment, professional training or admission to other educational establishments.

10.1.2 Current academic files are to be kept by the Academic Manager. Academic files may be consulted on a day-to-day basis by the Head of Programmes, the learners' own Tutor and Director of Studies, and authorized members of the administration. Academic files for past learners are held in semi-current storage and may be consulted by the Academic Manager and, with his/her permission. All other requests for access to an academic file must be authorised by the Head of Programmes or the relevant Director of Studies.

Data Area Contact: Academic Manager, Malta Business School

10.2 Learner admissions files

Admissions files are maintained in respect of candidates, and potential candidates, for admissions. During the admissions process such files are maintained and kept by the Head of Programmes, Admission Manager, and their authorized personnel. For successful candidates, the admissions documentation can be included in the Academic file. For unsuccessful candidates, the admissions documentation is retained for one year and then confidentially destroyed. During the admissions process, Admissions files may be consulted by the Head of Programmes, any of the Admissions personnel, the Director of Studies and any other interviewers. All other requests for access to an Admissions file must be authorised by either of the Admissions Manager or the Head of Programmes.

Data Area Contact: Head of Programmes, Admissions Manager, Malta Business School

10.3 Files in respect of any disciplinary matters involving learners

All such files are to be maintained and kept by the Academic Manager and Head of Programmes or his/her representative, who may each consult the same on a day-to-day basis. Sensitive information is placed in a sealed envelope in the learner's Academic File. Alternatively, such sensitive digital information is placed in a password protected file, or a file with accessibility levels available only to senior management. All requests for access must be authorized by the Academic Manager or representative.

Data Area Contact: Academic Manager, Malta Business School

10.4 Medical files in respect of learner health and welfare

Medical files are to be maintained and kept by the Academic Manager, who may consult the same on a day-to-day basis. All other requests for access to medical files must be authorised by the Academic Manager.

Data Area Contact: Academic Manager, Malta Business School

10.5 Medical notes in respect of learners

10.5.1 Such notes are maintained by the Academic Manager in the learner's Academic file for health and safety reasons, to assist in meeting the needs of learners with disabilities, or for reasons

connected with absences from School, accessibility issues, conditions affecting learning, poor performance, applications etc.

10.5.2 All current notes in this category are kept by the Academic Manager or representative. Sensitive information is placed in a sealed envelope in the learner's Academic File, or authorised access only digital files. The notes may be consulted on a day-to-day basis by the Academic Manager, the learners' own Tutor and the Academic Manager's representative. All other requests for access to these notes must be authorised by the Academic Manager.

Data Area Contact: Academic Manager, Malta Business School

10.6 Personnel files in respect of other employed staff of the School

10.6.1 These are maintained and kept by the Dean and Director of the School. These files may be consulted on a day-to-day basis by the Director or his representatives. All other requests for access to these files must be authorized by the Dean and Director.

Data Area Contact: Dean & Director

10.7 Wages files in respect of employed staff

These are maintained and kept by the Dean and Director of the School. These files may be consulted on a day-to-day basis by the Director or his representative. All other requests for access to these files must be authorized by the Dean and Director.

Data Area Contact: Dean & Director

10.8 Files relating to tenancies of the School's assets, suppliers of goods and services to the School, and other third parties not otherwise dealt with in this policy document

10.8.1 These are maintained and kept by the Finance Director. These files may be consulted on a day-to-day basis by the Finance Director or her representative. All other requests for access must be authorised by the Finance Director.

Data Area Contact: Finance Director

10.9 Learners' relations

10.9.1 Manual and computer based files are maintained in respect of current and former learners, and other current, past and potential learners of the School.

10.9.2 All files are kept locked and monitored and access to the computer database is password protected. The School's Administration may consult the manual and computer based files on a day to day basis, but requests by others to view these files must be authorised by the Head of Programmes.

10.9.3 Data will be used by the School for a full range of activities, including the sending of School publications, promotion of services available, notification of activities, and fund-raising programmes (which might include an element of direct marketing).

Data Area Contact: Head of Programmes, Malta Business School

10.10 Computer Databases

10.10.1 Some of the files referred to above are maintained in electronic rather than, paper files. Access to such databases is restricted in the same manner as access to paper files in the relevant Data Area.

10.10.2 In addition, however, the IT Systems Manager may have day-to-day access to the electronic databases for the purposes of administering and maintaining the same.

Data Area Contact: IT Systems Manager

11. Email

11.1 It is permissible and appropriate for the School to keep records of internal communications, which are relevant to an individual's ongoing relationship with the School, provided that such records comply with the Data Protection principles.

11.2 It is recognised that email is used for such communications and that such emails should form part of the School's records. It goes beyond the scope of this policy document to address the appropriate use of email in the proper functioning of the School, and the limitations and legal implications with this mode of communication. However, all members of the School need to be aware that:

- The 2001 Act applies to emails which contain personal data about individuals which are sent or received by members of the School (other than for their own private purposes as opposed to School purposes).
- Subject to certain exceptions, individual data subjects will be entitled to make a data subject access request and have access to emails which contain personal data concerning them, provided that the individual data subject can provide sufficient information for the School to locate the personal data in the emails; and
- The legislation applies to all emails from and to members of the School which are sent and received for School purposes, whether or not the emails are sent through the School email system or on an individual's own email account.

12. Sensitive Personal Data

12.1 The School may, from time to time, process "sensitive personal data" relating to admissions candidates, members and staff of the School.

12.2 Sensitive personal data is information as to a data subject's racial or ethnic origin, political opinions, religious beliefs or beliefs of a similar nature, trade union membership, physical or mental health or condition, sexual life, offences or alleged offences, and information relating to any

proceedings for offences committed or allegedly committed by the data subject, including the outcome of those proceedings.

12.3 Currently, the School envisages the need to process sensitive personal data of a type specified in the School's consent forms. For example, medical records need to be processed for the provision of healthcare and general welfare, to identify any necessary dietary requirements and to assist in meeting the needs of members of the School's Community with disabilities. In exceptional circumstances, the School may need to process information regarding criminal convictions or alleged offences in connection, for example, with any disciplinary proceedings or other legal obligations.

12.4 In other circumstances, where sensitive personal data is to be held or processed, the School will seek the explicit consent of the member of the School in question unless one of the limited exemptions provided in the Data Protection Act applies.

13. Data Security and Disclosure

13.1 All members of the School's Community are responsible for ensuring that:

- Any personal data which they hold is kept securely.
- Personal data is not disclosed either orally or in writing or otherwise to any unauthorised third party, and
- That every reasonable effort will be made to see that data is not disclosed accidentally.

13.2 *Unauthorised disclosure is a disciplinary matter and may be considered gross misconduct. If in any doubt, consult the School's Information and Data Protection Officer.*

13.3 Personal data must be kept securely and examples of how this may be done will include:

- Keeping the data locked in a filing cabinet, drawer, or room; or
- If the data is computerised, ensuring that the data is password protected or kept only on disk which is itself kept securely; or
- Any other appropriate security measure.

14. Candidates and Personnel obligations

14.1 Learners and Staff must ensure that any personal data provided to the School is accurate and up to date. They must ensure that any changes of address or other personal details are notified to the Dean and Director or one of his assistants.

15. Data Subjects' Consent

15.1 Certain types of personal data may be processed for particular purposes without the consent of individual data subjects. However, it is the School's policy to seek express consent whenever practicable from individual data subjects for the main ways in which the School may hold and process personal data concerning them. This is to allow individuals an opportunity to raise any objections to any intended processing of personal data. The School will consider any such objections but reserves the right to process personal data in order to carry out its functions as permitted by law.

15.2 Therefore, all prospective tutors, staff, admission candidates and learners will be asked to sign a consent form regarding particular types of information which the School may in due course hold/process about them.

16. Right to Access Personal Data

16.1 Staff, learners and other individuals have the right under the 2001 Act to access any personal data that is being held about them either in an "automatically processable form" (mainly computer records) or in a "relevant filing system" (i.e. any set of information structured in such a way that specific information relating to a particular individual is readily accessible) and to request the correction of such data where they are incorrect.

16.2 An individual who wishes to exercise his/her right of access to personal data is to file a Request to the School's Information and Data Protection officer.

16.3 Any inaccuracies in data that are noticed should also be communicated immediately to the Data Protection Officer who shall take appropriate steps to make the necessary amendments.

17. Disclosure outside of the EEA

17.1 The School may, from time to time, desire to transfer personal data to countries or territories outside of the European Economic Area in accordance with purposes made known to individual data subjects. For example, the names and contact details of the School's members of staff on a website may constitute a transfer of personal data worldwide. Accordingly, the consent form signifies an individual's consent to the inclusion of such data on an authorized School website. If an individual wishes to raise an objection to this disclosure then written notice should be made to the Information and Data Protection Officer.

17.2 Other personal data, even if it would otherwise constitute fair processing, must not, unless certain exemptions apply or protective measures taken, be disclosed or transferred outside the EEA to a country or territory which does not ensure an adequate level of protection for the rights and freedoms of data subjects.

18. Intellectual Property rights

18.1 All teaching sessions, recordings and materials written whether machine readable or otherwise, developed by or with the participation of Tutors and learners shall be the exclusive property of Malta Business School, and all and any rights that would otherwise vest in the Tutor under the Copyright Act 2000 (Act XIII of 2000) or under any other law or by-law shall vest in Malta Business School to the fullest extent.

19. Audio or video recording and/or live-streaming

19.1 Malta Business School collects personal data from recorded teaching sessions for specified, explicit and legitimate purposes. This data is not further processed in a manner that is incompatible with those purposes.

19.2 The processing of personal data of learners and tutors is permitted if the purpose of the processing is educational (such as teaching or assessment), regardless of whether the processing takes place via livestreaming or recording) and the processing constitutes a requirement for the teaching to be carried out. This takes place on the legal basis of legitimate interest of Malta Business School to carry out its teaching commitment.

19.3 The recording and then storage of such audiovisual material also entails data processing relating to the identity or other information relating to tutors and learners. The recording, storage and communication of such data shall be used by Malta Business School at its discretion in pursuit of its educational activities. All such data, including its processing, storage and use in the future is deemed necessary for the legitimate interests pursued by Malta Business School, which interests are of an educational nature, and within the terms of data protection legislation.'

20. Revisions

20.1 This Policy document will be the subject of an annual review and will be updated as circumstances and legislation change, to ensure that the Policy remains relevant.

This policy was last updated on 31.01.2024