SECTION 3: Data Protection

The Malta College of Arts, Science and Technology was established by public deed of the 11th August, 2000. Its function is incorporated in the Education Act, Cap 327, Part VIII. The MCAST's role is to '*To provide universally accessible vocational and professional education and training with an international dimension, responsive to the needs of the individual and the economy.*' (MCAST Mission Statement). In so doing, the College commits itself to handle personal and sensitive data in compliance with the General Data Protection Regulations (GDPR) that regulates the processing of personal information, whether held manually or electronically and also in compliance with the relevant requirements of the Education Act and subsidiary legislation.

Purposes for collecting data

MCAST collects and processes information to carry out it functions. All data collected and processed in accordance with GDPR, The Education Act, and any other subsidiary legislation.

Recipients of data

Personal information is accessed by MCAST staff who are responsible to carry out specific tasks as part of MCAST's functions. Disclosure may also be made to third parties, only in situations where this is mandated by law and/or where prior consent was obtained from the data subject.

Student and Staff rights

The rights and details of what type of information MCAST processes in the case of students and staff are described in the 'MCAST Privacy Policy Staff' and 'MCAST Privacy Policy Students' sections below.

Retention policy

MCAST will retain the information only as long as it is necessary, or as required by law. For more detailed information about retention periods for the various types of personal and sensitive data, refer to 'MCAST Retention Policy'.

The Data Protection Officer

The Data Protection Officer may be contacted at:
Mr Mario Pace
Malta College of Arts, Science and Technology
Data Protection Office
Administration Building
Corradino Hill
Paola. PLA9032
Malta
Telephone: 23987141
Email: dpo@mcast.edu.mt

3.1 Privacy Policy for Staff

3.1.1 Scope

The College is committed to protecting the privacy and security of personal and sensitive information. This privacy notice describes how the College collects and uses information about data subjects during and after their working relationship with the College, in accordance with the Data Protection Act (Chapter 440 of the Laws of Malta), as may be amended, and the General Data Protection Regulation (EU) 2016/679).

It applies to all data subjects including current and former employees and students and contractors.

The College is a "data controller". This means that the College is responsible for deciding how to hold and use personal information (i.e. "personal and sensitive data") about the data subjects. The College is required under applicable data protection legislation to notify data subjects of the information contained in this Notice.

Everyone essentially has rights with regards to the way and manner in which their personal and sensitive data is handled. During the course of its activities, the College will process personal and sensitive data as a data controller (which may be held on paper, electronically, or other medium) and recognises the need to treat it in an appropriate and lawful manner, in accordance with the Data Protection Act (Chapter 440 of the Laws of Malta), as may be amended from time to time, and the General Data Protection Regulation (Regulation (EU) 2016/679) (the "GDPR" or the "Regulation").

The purpose of this Notice is to set out the basis on which the College will process the personal and sensitive data, to inform the data subject about how the College will handle and look after personal and sensitive data and to explain (i) obligations in regard to processing personal and sensitive data responsibly, (ii) data protection rights as a data subject and (iii) how the law protects data subjects.

This Notice applies to current and former students and employees and contractors. This Notice does not form part of any contract of employment or other contract to provide work or services. This Notice may be updates or amended at any time.

It is important that data subjects read this Notice, together with any other privacy notice the College may provide on specific occasions when personal and sensitive data about data subjects is being collected and processed, so that data subjects are aware of how and why the College is using the data subjects' personal and sensitive data.

For identity purposes, the data controller is The Malta College of Arts, Science and Technology (MCAST) of Corradino Hill, Paola.

3.1.2 Definition of terms

Refer to Appendix 1.

3.1.3 Data protection principles

The College will use all efforts to ensure and maintain compliance with applicable data protection laws and principles. This means that the personal and sensitive data held by the College about its data subjects must be:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that have been clearly explained to data subjects and not used in any way that is incompatible with those purposes.
3. Relevant to the purposes explained by the College to the data subjects and limited only to those purposes.
4. Accurate and kept up to date.
5. Kept only as long as necessary for the purposes explained by the College.
6. Kept securely.

3.1.4 The kind of information the College processes about the data subject

As set out above, personal data (or personal information) means any information about a living individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data) or can no longer lead to identification (pseudonymised data). It also does not include information relating to a legal person (for example, a company or other entity). There are special categories of more sensitive data which require a higher level of protection.

The College collects and maintains different types of personal information in respect of persons who have an employment or working relationship with the College, including (in the case of employees) the personal information that was provided and obtained during the application and recruitment process.

The College will generally collect, store, and use the following categories of personal data:

- Personal details such as the data subjects' first name, surname, title and identity card or document number;
- Personal contact details such as the data subjects' home address (including post code), telephone number, mobile number and personal email address;
- Date of Birth;
- Gender;
- Marital Status and dependants;
- Spouse's name and identity card or document number (where applicable);
- Next of kin and emergency contact information;
- Social Security number;
- FS3 and FS4 Information (the completed mandatory form);
- Bank account details, payroll records and tax status information;
- Salary, annual leave, pension and benefits information (where applicable);
- Rate per hour in case of part time employment;
- Commencement date;
- End date where on a fixed-term contract;
- Employment or working status (full time, casual part time or visiting lecturer);
- Location of employment or workplace;
- The MCAST institute or department to which data subject has been assigned or otherwise engaged for;
- MCAST email account;
- Curriculum vitae (CV) and applicable qualification certificates;
- Assessment and performance reviews;
- Recruitment information (including references, interview notes and other information included in a CV or cover letter or as part of the recruitment process);
- Previous work history;
- Compensation history;
- Disciplinary and grievance information;
- Exit Interview (including questionnaire replies);
- CCTV footage and other information obtained through electronic means such as swipe and access card records;
- Entry and exit logs and security logs;
- Information about use by data subject of College information and communications systems.

The College may also collect, store and use the following sensitive data about its data subjects:

- Health information, such as physical conditions and disability status (please refer to Clauses 3.1.12-3.1.14 below to see how this information is used and reasons for doing so).
- Right to work documentation (where applicable);
- Court clearance searches and results.

3.1.5 Method of collecting personal information

Personal data about employees, students and contactors is collected through the application and recruitment process, either directly from candidates or sometimes from an employment or recruitment agency or background check provider, as well as from publicly-available information on professional networking sites.

The College may sometimes collect additional information from third parties, including former employers.

The College may also collect additional personal information about its data subjects in connection with their job or work related activities throughout the period of working relationship with the College.

3.1.6 How information is used

The College will only use personal data as allowed by the law. Most commonly, the College will use personal data in the following circumstances:
1. To perform the contract entered with the data subject.
2. In order to comply with a legal obligation.
3. Where it is necessary for the legitimate interests of the College or those of a third party and the data subjects interest and fundamental rights do not override those interests.
4. Upon data subject's consent (limited scenarios and for which the College will provide a consent notice).
5. Where the College needs to establish, exercise or defend any legal claims

The College may also personal information in the following situations, which are likely to be rare:

1. Where the College needs to protect the interests of the data subject (or someone else's interests).
2. Where it is needed in the public interest or for official purposes.

3.1.7 Situations in which the College will use personal data

The College needs the categories of personal information set out above in Clause 3.1.4 primarily to allow (the College) to perform its contract with the data subject and to fulfil its contractual obligations to its data subjects (such as the payment of salary or remuneration, as applicable), and to enable the College to comply with its legal obligations (for example, national insurance contributions in the case of employees).

In some cases, the College may use personal data to pursue its legitimate interests or those of third parties, provided the data subjects interests and fundamental rights do not override those interests. The situations in which the College will process the data subjects' personal data are listed below.

i. To perform the contract entered into with the data subject and the College's legal obligations
   - Checking that data subject is legally entitled to work in the EU;
   - Administering the contract entered with the data subject;
   - Paying data subject (payroll) and, in the case of an employee, deducting and paying tax and National Insurance contributions, as required;
   - Employee earnings reporting and maintaining employee records;
   - Conducting performance reviews, managing performance and determining performance requirements;
   - Managing sickness absence leave and assessing employee attendance;
   - Complying with health and safety obligations;
   - To comply with applicable employment laws and for tax, inland revenue and related purposes;
   - To comply with its legal obligations, as may be imposed on the College from time to time.

ii. Legitimate Interests
   - Recruitment and determining eligibility for initial employment or entry into a working relationship with the College;
   - Determining the terms on which to employ, hire or engage the data subject;
   - Liaising with the data subject's pension provider;

- Business management and planning, including accounting and auditing;
- Internal correspondence regarding job or work related activities;
- Making decisions about salary reviews and compensation;
- Assessing qualifications for a particular job or task, including decisions about promotions;
- Gathering evidence for possible grievance or disciplinary hearings;
- Making decisions about data subject's continued employment or engagement;
- Making arrangements for the termination of the employment or working relationship;
- (Continued) education, training and development requirements;
- To conduct data analytics studies to review and better understand employee retention and attrition rates;
- To reduce employee attrition rates;
- To prevent fraud and employee or worker abuse;
- Managing internal disputes between employees and/or workers;
- To ensure the security of College premises and property (namely, via CCTV footage);
- To ensure the security of the belongings and property of other employees, workers and contractors (namely, via CCTV Footage);
- To monitor, assess and ensure compliance with security policies,
- To ensure network and information security, including preventing unauthorised access to the College omputer and communications systems and preventing malicious software distribution;
- To pursue or exercise any other legitimate interests that the College may have at law;

iii. To establish, exercise or defend legal claims
- To deal with legal disputes which relate to or otherwise involve data subjects, or other employees, workers and contractors, including accidents at work.

Some of the above grounds for processing will overlap and there may be several grounds which justify use of personal information (the categorisation in this Clause 3.1.7 is mainly indicative). These grounds may be updated from time to time.

In all other cases, including marketing and advertising purposes, the College shall issue Consent Forms whereby the data subject shall be requested to consent to the processing by the College of the personal information for the purposes contained therein (e.g. where the College wishes to feature the data subject on the College newsletter and brochures). Such consent is entirely at the discretion of the data subject and withholding consent by the data subject shall not give rise to any adverse consequences on his/her job performance, career opportunities and advancements. Data subjects are requested to read these Consent Forms carefully before signing them.

The data subject is also entitled to revoke any consent which s/he may provide at any time by sending an email to dpo@mcast.edu.mt. This withdrawal of consent shall not affect any processing which may have taken place prior to such withdrawal. It shall also not affect any processing which is carried out by the College pursuant to another lawful basis.

3.1.8 Failing to provide personal information

If the data subject fails to provide certain personal information when requested, the College may not be able to perform the contract entered with the data subject into with the data subject (such as paying remuneration), or the College may be prevented from complying with its legal obligations (such as to ensure the health and safety of its workers).

3.1.9 Change of purpose

The College will only use personal data for the purposes for which it was collected, unless the College reasonably considers that it needs to use it for another reason and where that reason is compatible with the original purpose. If the College needs to use personal data for an unrelated purpose, the College will notify the data subject and the College will explain the legal basis which allows the College to do so.

The College may process personal data without the need to obtain consent, in compliance with the above rules, where this is required or permitted by law.

3.1.10 How sensitive data is used

Sensitive data requires higher levels of protection. The College therefore needs to have further justification for collecting, storing and using this type of personal information.

The College may process sensitive data:
1. In limited circumstances, with the data subjects explicit written consent.
2. Where the College needs to carry out its legal obligations or exercise rights in connection with employment.

Less commonly, the College may process this type of information where it is needed in relation to legal claims or where it is needed to protect the data subjects interests (or someone else's interests) and the data subject is not capable of giving consent, or where the data subject has already made the information public.

3.1.11 Obligations of the College as regards to requiring consent

The College does not need the data subject's consent to use sensitive data to strictly assess the data subject's working capacity, to carry out its legal obligations or exercise specific rights in the field of employment law (This applies in relation to Clauses 3.1.12-3.1.15 below).

In limited circumstances, the College may approach the data subject for his/her written consent to allow the College to process certain, particularly sensitive data. If the College does so,the College will provide the data subject with full details of the information that the College requires like and the reason it is needed, so that the data subject can carefully consider whether h/she wish to consent or not. The data subject should be aware that it is not a condition of the data subject's contract with the College to agree to any request for consent from the College. The data subject may also withdraw his/her consent at any point in time.

3.1.12Health Information

The College shall only process sensitive data relating to the data subject's health (health data) strictly in accordance with the provisions and requirements of Article 9 of the GDPR. This provides that processing of sensitive data relating to the health of employees may be carried out under the responsibility of a Healthcare Professional and for the assessment of the working capacity of the employee. Healthcare Professionals are subject to professional secrecy obligations in line with applicable Maltese laws.

Additionally, the data subject may also freely decide to provide the College (at the data subject's discretion) with information about:

- any physical conditions that the data subject may suffer from (such as allergies); and
- where the case, the disability status that may be applicable to the data subject.

The College will only process and use any such information that it receives from the data subject strictly for the purposes stated in Clause 3.1.10 and 3.1.11 above.

3.1.13 Medical Records

Furthermore, employees are required to provide the College with a medical certificate, issued by a registered medical practitioner, where they take more than two (2) days' leave from work due to sickness (sick leave). The College processes these medical certificates in order to confirm that the sick leave was legitimately exercised by the employee and that there has been no abuse on the part of that employee, to also comply with the College's specific obligations under, in particular, the Minimum Special Leave Entitlement Regulations (S.L. 425.101) or under the applicable Wage Regulation Order (together, the "Regulations") and (where the College suspects employee abuse) to detect the existence of any sick leave patterns and trends by the employee concerned. The College is entitled under the Regulations to request and receive this documentation from the data subject (unless excluded by an applicable collective agreement).

Medical certificates for sick leave absences which may be required to be presented to the College, or which the College may be obligated or entitled at law to collect (as mentioned above), shall be treated in the utmost confidentiality and retained in a designated cabinet with limited access solely to the Human Resources staff who shall not share this information with other members of the management team, co-employees or, needless to say, any third parties.

3.1.14 How health information is used

The College will use information relating to leaves of absence, which may include sickness or family-related absences, to comply with employment and other laws (including the Regulations), to exercise the College's rights under the Regulations (as an employer) as well as for the purposes stated in Clause 3.1.13 above.

Health information will only be processed by the College, at all times under strict confidentiality, if there is the need to ensure health and safety in the workplace of the data subject or co-workers, to provide appropriate workplace adjustments, to monitor and manage absences from work due to sickness, and to apply and administer benefits to the data subject or on the data subject's behalf (for example, disability benefits).

3.1.15 Police conduct certificates

The College will generally require the data subject to provide the College with a clean police conduct certificate in order to be in a position to confirm the data subject's appointment. A note of the results of the certificate will be retained as part of the data subject's HR file during the course of the data subject's working relationship with the College. The College does not keep copies of the certificate itself.

3.1.16 Court clearances

The College has a legal obligation by virtue of the Protection of Minors (Registration) Act (Chapter 518 of the Laws of Malta) (the "Act") to carry out a so-termed "court clearance search" on any individual that it either intends to employ or to otherwise entrust with a position at its institution. This is due to the fact that minors (as defined under applicable Maltese laws) form part of its student base.

This court clearance search entails filing an application to the Court of Voluntary Jurisdiction of the Maltese Civil Courts requesting the Attorney General of Malta to carry out a search on the relevant individual in a register maintained by the Registrar, Civil Courts and Tribunals, in terms of Article 3 of the Act. The relative application is prepared and submitted by a lawyer acting on the College's behalf and will be served on the Attorney General. Once the searched has been carried out, the Attorney General will be required to file its reply regarding the results of the search and the Court will then issue its decree based

on those results. This decree will be communicated to us, typically through the College's lawyer. The information to be disclosed in the decree (which may or may not include information about possible offences committed by the individual) is solely identified and determined by the Court.

The College does not retain the decree issued by the Court, including where it discloses information about prior offences. In the case of a positive decree (i.e. no results), the Collge will merely take a note of the outcome of that decree, which will be retained as part of the data subject's HR file during the course of his/her working relationship with the College. This note is kept and maintained in the strictest confidence at all times, and will only be accessible to the principal and HR staff. However, in the case of a negative decree, the College:

- will firstly not be in a position at law to employ or otherwise engage the data subject; and
- will also be bound to adhere to any orders or directives which may be issued by the Court.

[In such a case, a note will be taken and logged that the College was not able to employ or engage the data subject. This note will be equally kept and maintained in the strictest confidence at all times, will only be accessible to the Principal and HR staff, and will only be used for the following limited purposes:

- for any subsequent employment or work application which the data subject may lodge with the College; and
- for use in any legal claims that the data subject may file against the College in connection with the decision of the College not to employ or otherwise engage the data subject].

The College will entrust and engage a lawyer to handle this process on the College's behalf, as indicated above. For the purposes of the required Court application, the lawyer will generally need to be provided with the following details about the data subject: name, surname, identity card or document number, and commencement date. Moreover, the lawyer will also be privy to the Court decree and the information contained in it, as well as any information which could potentially be disclosed during a hearing on the application (if appointed by the Court). Note that lawyers are subject to strict professional secrecy obligations in line with applicable Maltese laws.

3.1.17 Data sharing

The College may have to share personal data with third parties, including third-party service providers and professional advisors. The College will require third parties to respect the security of the data and to treat it in accordance with the law.

3.1.17.1 Third-party service providers processing personal information?

"Third parties" includes third-party service providers (including contractors, professional advisors and designated agents) and public authorities.

The following activities are carried out by third-party service providers: legal counsel, security services and cleaning.

3.1.17.2 Securing information with third-party service providers

All the College's third-party service providers are required to take appropriate security measures to protect personal data, in line with College policies. The College does not allow third-party service providers to use personal data for their own purposes. The College only permits them to process personal data for specified purposes and in accordance with the College's explicit, written instructions. They are contractually bound by appropriate agreements in respect of any and all processing of the personal data.

3.1.17.3 Third parties

The College may also need to share personal data with a regulator, a public authority or law enforcement

authorities or to otherwise comply with the law. The College is obligated under the Protection of Minors (Registration) Act (Chapter 518 of the Laws of Malta) to disclose the commission of a scheduled offence (as defined by that Act) which occurs at the College's institution to the Commissioner for Police.

3.1.18 Data security

The College has put in place measures to protect the security of information. Details of these measures are available upon request. Third parties will only process personal data on the instructions of the College and where they have contractually agreed to treat the information confidentially and to keep it secure.

The College has put in place appropriate security measures to prevent personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

In addition, the College limits access to personal information to the Principal, Deputy Principal Corporate Services and strictly only those employees, agents, contractors and other third parties who have a business need to know. They will only process personal information on the College's instructions and they are subject to a duty of confidentiality.

Details of these measures may be obtained from the Data Protection Officer.

The College has also put in place procedures to deal with any suspected data security breach and will notify the data subjects and any applicable regulator of a suspected breach where the College is legally required to do so.

Whenever possible, and where it is not necessary, or otherwise no longer necessary, to identify the data subject, such as for research or internal analysis purposes, the College will pseudonymise or anonymise personal data so that it can no longer be used to identify the data subject.

3.1.19 Transferring of personal data to a country outside the EEA

The College ay transfer any held personal data to a country outside the EEA provided that:

- the country to which the personal data is transferred ensures an adequate level of protection for the data subject's rights and freedoms recognised under EU data protection law;
- in the absence of an adequacy decision, the data transfer is regulated by specific contracts approved by the European Commission which afford personal data the same standards of protection it has in Europe;
- the transfer is necessary for the performance of the data subjects' employment contract with the College;
- the transfer is necessary for the performance of a contract concluded in the data subjects' interests between the College and another person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary in order for the College to comply with a legal or regulatory obligation; or
- the transfer is necessary for the filing, or defence, of legal claims.

For all other cases, the College will request the explicit consent of the data subject to transfer data outside the EEA.

3.1.20 Data retention

3.1.20.1 Retention Period

The College will only retain personal data for as long as necessary to fulfil the purposes the College

collected it for, including for the purposes of satisfying any legal, tax, accounting, or reporting requirements. This means that data will be destroyed or erased from the College's systems when it is no longer required.

To determine the appropriate retention period for personal data, the College considers the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of personal data, the purposes for which the College processes personal data and whether the College can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances, the College may anonymise personal data so that it can no longer be associated with the data subject, in which case the College may use such data without further notice to the data subject. Once the data subject is no longer an employee, worker or contractor of the College, the College will retain and securely destroy personal data in accordance with the data retention policy.

Refer to Section 3.4

3.1.21 Rights of access, correction, erasure, and restriction

The data protection laws across the EU, including Malta, changed on 25th May, 2018, due to the application of the GDPR.

3.1.21.1 Duty by data subject to inform of changes

It is important that the personal data held by the College is accurate and current. The data subject is required to keep the College informed if the data subject's personal data changes during the working relationship with the College.

3.1.21.2 Right of Access

The data subject has the right to request information as to whether or not the personal data is being processed by the College, as well as information as to how and why it is being processed.

The data subject may send an email to dpo@mcast.edu.mt requesting information and a copy of the personal data processed by the College. The data subject shall receive one copy, free of charge and via email, of his/her personal data which is undergoing processing by the College. A limit of two such requests per 12 month period is being made for logistical reasons.

This right to access one's personal data is without prejudice to the integrity and confidentiality of the personal data of other persons, and only data which is solely related to the data subject can be divulged.

3.1.21.3 Right to Correction

The data subject has the right to request correction or rectification of the personal data that is held at the College. This enables the data subject to have any incomplete or inaccurate data that the College holds the data subject corrected and/or updated, though the College may need to verify the accuracy of the new data provided to the College by the data subject.

3.1.21.4 Right to Erasure

The data subject has the right to request erasure of his/her personal data. This enables the data subject to ask the College to delete or remove personal information where there is no good reason for the College continuing to process it.

The data subject also has the right to ask the College to delete or remove the data subject's personal information where the data subject has exercised his/her right to object to processing (see below).

Note, however, that the College may not always be able to comply with the data subject's request of erasure for specific legal reasons which will be notified to the data subject, if applicable, at the time of the data subject's request. Most commonly, this will be where further processing of the personal data is required by the College to:

- Comply with a legal obligation to which teh College is subject;
- assert, exercise or defence of legal claims (including possible future claims).

3.1.21.5Right to Object

The data subject has the right to object to processing of his/her personal data where the College is relying on a legitimate interest (or those of a third party) and there is something about the data subject's particular situation which makes the data subject want to object to processing on this ground. The data subject also has the right to object where the College is processing the data subject's personal data for direct marketing purposes.

3.1.21.6Right to Restriction

The data subject has the right to request the restriction of processing of his/her personal data. This enables the data subject to ask the College to suspend the processing of personal information about him/her, for example if the data subject wants the College to establish its accuracy or the reason for processing it.

3.1.21.7Right to Request Transfer (Data Portability)

The data subject has the right to request the transfer (data portability) of his/her personal data to him/her or to a third party. The College will provide to the data subject, or a third party chosen by the data subject the personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which the data subject initially provided consent to the College, or where the College used the information to perform a contract with the data subject.

3.1.21.8Exercise of Rights

If the data subject wants to review, verify, correct or request erasure of his/her personal data, object to the processing of his/her personal data, or request that the College transfers a copy of his/her personal data to another party, the data subject is to contact the Data Protection Officer in writing.

3.1.21.9 Requirements from the data subject

The College may need to request specific information from the data subject to help the College confirm his/her identity and ensure the right to access the information in question (or to exercise any other rights of the data subject). This is another appropriate security measure to ensure that personal data is not disclosed to any person who has no right to receive it.

3.1.21.10 Right to withdraw consent

In the limited circumstances, where the data subject may have provided consent to the collection, processing and transfer of personal data for a specific purpose, the data subject has the right to withdraw consent for that specific processing at any time. To withdraw consent, the data subject is to contact the Data protection Officer at dpo@mcast.edu.mt. Once the College has received notification that s/he has withdrawn consent, the College will no longer process information for the purpose or purposes originally

agreed to, unless the College has another legitimate basis for doing so in law.

3.1.22 Data protection officer and complaints

The College has appointed a Data Protection Officer (DPO) to oversee compliance with this Notice. If teh data subject has any questions about this Notice or how the College handles personal information, the data subject is required to contact the DPO on dpo@mcast.edu.mt. The data subject has the right to lodge a complaint at any time to the competent supervisory authority in his/her jurisdiction on data protection matters.

In the case of Malta, this is the Information and Data Protection Commissioner ("IDPC") (https://idpc.org.mt/en/Pages/Home.aspx). The College would, however, appreciate the opportunity to deal with any concerns internally before the data subject approaches the supervisory authority. The data subject is therefore invited so please bring the matter to the attention of the College at the first instance.

3.1.23 Changes to this privacy notice

The College reserves the right to update this Notice at any time, and will provide the data subject with a new privacy notice when the College makes any substantial updates. The College may also notify the data subject in other ways from time to time about the processing of personal information.

All queries are regarding this policy are to be addressed to the Data Protection Officer at dpo@mcast.edu.mt.

Appendix 'A'

In order to ensure that no personal data is accidentally leaked from MCAST, the following procedures are being implemented across all MCAST and applicable to all staff.

1. Employees are to save all their files exclusively and solely on MCAST servers and not local hard drive. MCAST reserves the right to block access to the local drives on its computers if the DPO deems it necessary with the approval of the Principal
2. In line with the above clause 1, the College will not grant access to any member of staff to save any information found on MCAST servers on external storage, be it pen drives, external hard drives or any other device. In line with the strict and utmost efforts being made by MCAST to save and protect all information and data found on its servers, only limited exemptions to this rule will be permitted by the PO upon approval by the Principal.
3. Again in line with the above rule and in conformity with the predominant rule that all data is to remain exclusively on the MCAST servers, any employee is forbidden from downloading any data, whether through email or otherwise, onto his/her own device, be it mobile, computer, tablet etc. To this effect, it is also being made clear that any data on the MCAST servers will be accessed by any employee's personal device if such device is secured with enabled encryption.
4. An MCAST employee shall not re-create lists which are already in existence as this will make it more difficult to delete all versions of that information when required.
5. An MCAST employee shall not give any information about MCAST, its staff, or its students to anyone (including but not limited to Government departments and agencies) without prior clearance from the Data Protection Officer or any other person delegated by him.
6. An MCAST employee shall not collect photocopies of ID cards, passports or police conduct certificates. The data subject may ask to see them to verify the contents therein but they are to be returned to their owner immediately. Any photocopies of such documents already in the data subjects' possession should be destroyed (shredded) immediately.
7. An MCAST employee shall not put people on any mailing list without obtaining their consent beforehand and these are to be removed from any such mailing lists as soon as the consent is revoked.
8. Age of consent with regards to education purposes is 16, not 18. If parents ask for information about their children, they need to come in person accompanied by their children, and such information can only be given if the children give their consent. The only exception to this is those students who are still under the age of 16 (normally such occurrences only happen between October and December only).
9. Under no circumstance shall any information about anyone be given over the telephone or through an email, since the true identity of the recipient cannot be verified in that manner.
10. Staff at Institutes are to ensure that they have two separate student files, one for personal information and one for sensitive information (medical, psychological etc). The personal files can be kept at the SAO filed in lockable cabinets, whilst the sensitive information files are to be kept under lock and key in the directors' (or deputy directors) office.
11. Any research that uses personal information about staff and/or students should be default be anonymised before used by researchers. In particular instances where MCAST feels that the results of the research could help individual students in their stay at MCAST and beyond, the data can be pseudo-anonymised by MCAST and key should never be made available to the researchers.