etb

Bord Oideachais agus Oiliúna
Mhaigh Eo, Shligigh agus Liatroma
Mayo, Sligo and Leitrim
Education and Training Board

GDPR Manual

A practical guide for schools and centres

MSLETB Corporate Services, March 2019

Table of Contents

1. Introduction

The purpose of this document is to provide guidance for school staff and those working in Further Education and Training centres in Mayo, Sligo and Leitrim Education and Training Board ('MSLETB') in respect of the *General Data Protection Regulation* (EU) *2016/679* ("GDPR") . The Regulation came into force on the 25th May 2018 and introduced increased obligations for both data controllers ('**Controllers**') and data processors ('**Processors**').

1.1 Definitions

Personal data

The term 'personal data' means any information relating to a living person who is identified or identifiable. This person is referred to as a 'data subject'. If the information can be used on its own or in combination with other information to identify a specific person, then it counts as personal data.

The GDPR gives examples of identifiers which includes names, identification numbers, and location data. A person may also be identifiable by reference to factors which are specific to their identity, such as physical, genetic or cultural factors.

Special categories of personal data

Certain types of personal data are subject to additional protection under the GDPR. They are described under Article 9 of the GDPR as 'special categories of personal data' (previously known as sensitive data). The special categories are:

(i) personal data revealing racial or ethnic origin,
(ii) political opinions,
(iii) religious or philosophical beliefs,
(iv) trade union membership,
(v) genetic data and biometric data processed for the purpose of uniquely identifying a natural person,
(vi) data concerning health,
(vii) data concerning a natural person's sex life or sexual orientation.

Processing of these special categories is prohibited, except in limited circumstances as set out in Article 9 of the GDPR.

Data Protection Officer (DPO)

In MSLETB, this is the Head of Corporate Services.

Data Access Requests (DAR)

An individual has the right to access the information that an organisation holds about them. Accessing personal data in this way is known as making a ‘Data Access Request’ (sometimes also known as a ‘Subject Access Request’).

Processing

The term ‘processing’ refers to any operation or set of operations performed on personal data. Processing includes storing, collecting, retrieving, using, combining, erasing and destroying personal data, and can involve automated or manual operations.

Data Controller

A ‘data controller’ refers to a person, company, or other body which decides the purposes and means of processing personal data.

Data Processor

A ‘data processor’ refers to a person, company, or other body which processes personal data on behalf of a data controller.

Data Breach

A personal ‘data breach’ is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Data Protection Impact Assessment (DPIA)

A DPIA must be carried out <u>before</u> any new high risk processing project. This assessment is used to identify and mitigate against any data protection related risks arising from a new project which may affect your organisation or the individuals it engages with.

Data Processing Agreement (DPA)

A DPA is a legally binding contract where a Data Controller engages a Data Processor to process personal data on their behalf. It sets out, amongst other things, the terms and conditions of how data is being processed and how it can be used.

2. GDPR – General Guidance for all Staff

2.1 General

- Exercise good judgement and professionalism in note taking. Anything that you write about a student or learner can be requested by that person under data protection legislation and/or under the *Freedom of Information Act 2014* (FOI).
- Ensure that staff members only have access to personal data on a need-to-know basis.
- Consider audibility through stud walls, doors, open windows, etc. Do not discuss personal information where you may be overheard.

2.2 Special Category data[1]

- Take extra care when handling special category data as greater legal restrictions apply. Keep it locked with access restricted to a 'need to know' basis.
- Be vigilant with emails and attachments, particularly when dealing with special category data. Always password protect documents when sending special category data (Please see Appendix 1 for information on password protecting and encrypting documents).

2.3 Lost, stolen or shared incorrectly data

- If data is lost or stolen or shared with an unintended recipient, or a risk of loss / theft / improper sharing of data is identified, contact the DPO immediately.

  The DPO must communicate the data breach to the Data Protection Commissioner within 72 hours.

2.4 Emails

- Be aware of suspicious emails, particularly ones containing links. Do not enter your username or password anywhere unless it is deemed absolutely necessary to do so.
- Use strong passwords and change them regularly. Never share log-in credentials. Never allow someone else to see the password being entered.
- Prepare emails with high levels of diligence, ensuring that the correct email address is entered. Use "bcc" instead of "to" field when sending group emails. (see Appendix 2).

[1] Previously known as Sensitive Data, refers to any data containing information on racial or ethnic origin, political opinions, religious or philosophical beliefs, PPS Number, trade union membership and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural persons sex life or sexual orientation

Password protect emails where appropriate. Please see Appendix 3 for data protection guidance on email queries.

- Do not access work email or system accounts from personal electronic devices. Please note that contents of e-mails are considered official records that can be monitored at any time.
- Include the school/centre name and address in your signature.

2.5 Proof of Identity

- No staff member may misrepresent himself / herself as another individual. This includes using another staff member's username and password.
- Staff must satisfy themselves as to the identity of callers i.e. verify date of birth or personal public service number prior to discussing any personal information over the phone. (Please see Appendix 7 for Data Protection Guidance on Telephone Queries)

2.6 Shredding

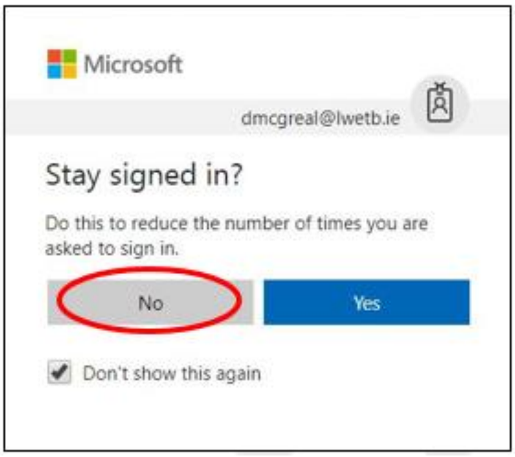
- Use cross-cut shredders/shredding company for disposal of paper records containing personal data when no longer needed. Contact the Corporate Services department for details of current provider.
- Avoid the use of 'for shredding' boxes. Documents should be shredded immediately or kept secure until shredded. The same applies to shredding bags (full or partially full) from a shredding contractor.

2.7 Use of Electronic Devices

- Electronic devices such as laptops, mobile phones and tablets that store personal data must be encrypted and kept locked when not in use.
- The use of USB devices to store personal data without encryption is prohibited. Non-MSLETB approved removable media such as CD, DVD, USB drive or SD cards etc. that contain data or files should NOT be used without consulting with IT Support.
- Removable media, being small items by nature, are easy to lose and leave behind. For this reason, their use is discouraged.
- Be aware of metadata[2] retained when creating, updating or modifying a document. Remove metadata for your own privacy. (See Appendix 4 for information on removing metadata on Microsoft word).

[2] Metadata provides information on the description and context of the data, for example, who created it and details of modifications.

- The use of a fax machine to send documents containing personal data is not recommended. If it must be used ensure that documents are sent to the correct number and that you arrange for the recipient to be waiting at the machine.
- Delete scanned documents that are no longer required.
- The use of online chatrooms either on the MSLETB/Office 365 network or outside of it is forbidden.
- The use of apps and web-based programs other than those provided by the MSLETB Office 365 software must be approved by the DPO prior to use. The use of student personal data on any apps must be strictly limited.
- Ensure you log out from all apps and web-based programs when you have completed your task.
- Never click 'Yes' when an app or computer program offers you the opportunity to 'remember' your password for you. Please refer to the following picture:



Stay signed in?

Do this to reduce the number of times you are asked to sign in.

☑ Don't show this again

2.8 Computers

- Lock your computer every time you step away from it using the keystroke combination (⊞ + L).
- Change your password to a passphrase (e.g. *Iarriveatworkbynineeachmorning*). Never share it with anyone. Never write it down.
- Ensure monitors are facing away from public view in places such as reception areas, open plan offices, public transport etc., especially when working with personal data to reduce the risk of others looking at your work, so-called 'Visual Hacking.'

2.9 Using your own device

- Store sensitive information on your OneDrive or in your MSLETB email account but do not sync either with your personal device. Only access your work emails/OneDrive via outlook.office365.com or via the 'Staff email' link on the school homepage, and not through local copies or app versions of these programs.

- Never accept a pop-up offer to download an app version of Office 365/ Outlook/ OneDrive/ VSWare, or a pop-up offer to allow your device to remember your password. Doing so will remove another line of security defence to whatever data is in those applications.

2.10 VSWare

- Keep the computer screen facing away from students.
- Make sure the connection with the projector is broken when reading or updating student's information.
- Record student attendance accurately as this will be part of the student's permanent school record.
- Log-off from VSware when you have completed your task.

2.11 Acceptable Usage

- All equipment provided by MSLETB remains the property of MSLETB.
- MSLETB Staff should be aware that the use of school technology including email/internet for personal use is not private. MSLETB retains the right to monitor such usage where it is considered to be in contravention with MSLETB's policies and ethos.
- Users of school email accounts should be aware that emails are considered 'records' which may be released under the Freedom of Information Act 2014.
- All personal data stored on MSLETB mobile devices must be protected by encryption software. All queries in respect of encryption should be directed to MSLETB IT Support.

2.12 Viruses

- Viruses can enter an organisation in several different ways such as unscanned digital storage media (e.g. CDs, DVDs, USB memory sticks, floppy disks being brought into the organisation).
- E-mails or attachments.
- Downloaded data from the Internet.

2.13 Internet

- Internet usage must be linked to your work and may be monitored on a systematic basis and as deemed necessary by MSLETB.
- Internet use to pay for, advertise, participate in or otherwise support unauthorised or illegal activities, is prohibited.

3. Guidance for Principals / Deputy Principals / Centre Managers

3.1 General

- Apply and enforce the ETB policies, which can be found on MSLETB's website at http://mayosligoleitrim.etb.ie/ under policies and procedures.
- Drive privacy and data protection awareness, ensure all records (electronic and manual) are stored securely with restricted access on a 'need to know' basis.
- Apply local procedures and protocols in line with MSLETB policies.
- Take appropriate preventative actions to mitigate the risk of data breaches arising.
- Prior to any new data gathering or processing activity (e.g. use of new web service or app, or anything involving a new use of student data, installation of CCTV), contact Corporate Services as a Data Protection Impact Assessment (DPIA) may need to be carried out first. Please see sample DPIA at Appendix 5.
- Carry out due diligence of service providers (data processors) prior to any service being retained.
- Ensure appropriate written contracts and data processing agreements are in place with all relevant service providers.
- Oversee Data Access Requests (DARs) and seek advice from Corporate Services where appropriate. Please see sample DAR Form at Appendix 6.
- Be vigilant in the security of school buildings (locking doors, locking gates etc.). Only a small number of designated staff should be able to open and lock up the school. Ideally, this should be limited to the Caretaker, Principal and Deputy Principal.
- Be aware that in investigations, disciplinary meetings and Section 29[3] hearings, any corroborating evidence considered must not contain identifiable data of other students. Unfortunately, this may adversely affect the weight and credibility of evidence submitted.
- Contact the DPO in the event of a data breach.

3.2 VSWare

- Ensure the correct access is given to members of staff. By default, teachers should now only be able to access their own student's information and not the information of students that they do not teach.
- Ensure that access for individual teachers is on a need-to-know basis only. For example, teachers will not always need access to the household tab for all students.

[3] As provided for in the Education Act 1998

3.3 CCTV

- Familiarise yourself with MSLETB's CCTV Policy.
- Footage should not to be kept any longer than 28 days, unless there is legal basis to hold on to it for longer.
- Keep CCTV monitors in a secure location with restricted access.
- Keep the password to access the recordings secure and with adequate standards of complexity and change it regularly.
- Internal cameras should be in corridors, reception and common areas only.
- Ensure no public areas are monitored beyond the perimeter of the school.
- Ensure appropriate CCTV signs are displayed in areas where CCTV is in operation, signs must include the following; who controls the CCTV system, purpose of CCTV, contact information.
- If installing a new CCTV system, replacing an old one or altering the existing system, contact Corporate Services as a **Data Protection Impact Assessment** may need to be carried out.
- If a security company is involved in monitoring the CCTV system, ensure that there is a Data Processing Agreement in place.

3.4 Data Access Request – When an individual requests a copy of their data

- Once a Data Access Request (DAR) has been received, establish if the information can be processed under Access Request Policy, under the Policies and Procedures tab of the MSLETB website. If the information cannot be processed in this manner, please contact Corporate Services for advice on the appropriate protocol.
- If a DAR is received, data gathering must be completed promptly as the deadline to reply to a DAR is one calendar month after receiving the request.
- Be aware that CCTV recordings may be subject to DARs.
- DARs must be made by the data subject. However, in certain circumstances, parents can make DARs on their child's behalf for example if the child is deemed too young to look after their own affairs or they have consented to their parents requesting a DAR on their behalf.
- Under Section 9 of the *Education Act 1998*, parents/guardians have the right to receive information about the student's educational progress until the student reaches the age of 18.

3.5 Request from other organisations (e.g. Tusla, Gardaí)

- Handle requests for information from bodies such as Tusla and the Gardaí with care. Such requests should be submitted in writing on official headed paper or from an official email address. If unsure of any request, contact Corporate Services.
- Do not divulge information over the phone or engage in informal 'confidential' conversations without being satisfied of the legal standing to such a request and confirmation of the identity of the caller.

3.6 Records Retention Schedule

- Assign an individual to be responsible for the secure disposal and deletion of records annually. This applies to paper and electronic records.
- **Note**: Ensure that you record anything that is destroyed in line with MSLETB's Record Retention Schedule listed under the Policies and Procedures on the MSLETB website.

4. Guidance for Teachers / Tutors

4.1 Paper records

- Ensure documents that contain student information are locked in a secure location when not in use or unattended, especially when working in a shared space.
- Notice boards: take care when displaying any personal data on notice boards, especially if these are visible to the public.
- If bringing work home, for example when marking exam papers/homework, ensure that the documentation is secure and not retained longer than necessary.
- Never share personal information contained in a list where other students' personal data appears. Third party personal data must be redacted.
- When recording data, for example minutes of meetings for broader circulation, consider the need to anonymise.

4.2 Exam papers / coursework / homework

- These documents must be retained in compliance with the school's policy and MSLETB Record Retention Schedule. These documents contain personal data and must be returned to students, filed as appropriate or shredded when they are no longer needed.
- Exam results and coursework must only be divulged to the student, and their Parent or Guardian if they are under 18.

4.3 Staff diaries

- Where the school provides a diary/yearbook/journal remember this is the school's property and must only be used for work purposes.
- Use of personal diaries for work purposes, or to store personal data relating to students, is prohibited.
- Do not use school diaries for personal entries.
- Do not leave staff diaries unattended — always keep them in a secure location.

4.4 Recording a student leaving early / arriving late

- When recording the attendance detail of a student, ensure that no personal details or specific reasons for an individual leaving early/arriving late is visible to anyone else.

4.5 Verbal Communication

- Personal data should not be discussed with or disclosed to anyone other than the person in question and/or parents, guardians and relevant professionals as appropriate.
- Never discuss or share a student's school work or results with other students or third parties.
- Never discuss or share a student's personal circumstances with other students or third parties.

4.6 Data protection on phone calls

- When taking a note of contact details over the phone, make sure that it is used as a temporary record and then destroyed e.g. calling someone back.
- For further guidance on phone calls, see Appendix 7 (Data Protection Guidance on Telephone Queries).

4.7 Photographs

- Ensure that you have consent before using or displaying students' photos / videos in the school's website, newsletter and noticeboards. Additional consent is required if a student's photograph and name is being published in newspapers. Ensure that the most up to date consent form is in place for each student.
- Photos/videos taken by parents/students with their own personal devices are not under the remit of Data Protection law.

5. Guidance for Receptionist / School Secretary

- Apply a clean desk policy (i.e. do not leave open documents/files on your desk which could potentially be seen by students or members of the public).
- Ensure that personal data is not visible to others.
- Keep personal data out of view of visitors, ensure that computer screens are not visible to others in the vicinity.
- Do not discuss personal information where you may be overheard. Consider audibility through stud walls, doors, open windows, etc.
- If a book or list is held on reception for the purpose of recording a student leaving early/arriving late, make sure no personal details or specific reasons are visible to anyone else. If a specific reason needs to be recorded, e.g. 'medical appointment', make sure it is treated as confidential data.
- Exercise diligence and attention-to-detail when entering data on to the school administrative system. Keep all data accurate, complete and up-to-date.
- Prepare post with careful attention to detail. Develop post protocol such as double checking that the correct letter is in correct envelope, correct enclosures, correct address, envelope securely sealed etc. If posting documents containing personal data, ensure that it is sent by registered post.
- Ensure that all Data Access Requests (DARs) are immediately brought to the attention of the Principal without delay. Be alert to the possibility of impersonation, trickery, deception, phishing, or social engineering.
- Exercise caution where an email requests that you click on links or open an attachment to a document.
- Respect access-permission levels and never view files or records where there is no genuine employment reason for doing so.
- Immediately notify the Principal if anyone attempts to obtain unauthorised access to personal data.
- Adhere to all school policies and protocols.
- Do not use a personal phone to contact parents, students or other staff in a professional capacity.

6. Guidance for Caretakers

- Be vigilant in the security of school buildings, such as locking doors and gates. Only a small number of designated staff should be able to open/lock up the school. Ideally, this should be limited to the Caretaker, Principal and Deputy Principal.
- Ensure that only authorised persons have access to school buildings.
- Ensure alarms are switched on and working.
- Ensure that CCTV systems are working, maintained and serviced appropriately.
- Store confidential wastepaper securely until it is securely shredded.
- Report any personal data breaches immediately to the Principal, including a situation where a letter /note containing personal data is found on school grounds.
- Comply with and give assistance during audits, spot-checks and inspection of school grounds.

7. Guidance for other Staff (Guidance Counsellor, SNAs etc.)

- Adhere to ethical standards required by professional, regulatory and representative bodies (for example the Institute of Guidance Counsellors).
- Exercise professional judgement in deciding what personal data can be shared and with whom e.g. child protection, child welfare, medical needs, DLP, Tusla, An Garda Síochána.
- Take responsibility for keeping sensitive data safe and secure (encryption, pseudonymisation, etc.).
- Exercise good judgement in note taking.