cmetb

Bord Oideachais agus Oiliúna
an Chabháin agus Mhuineacháin
Cavan and Monaghan
Education and Training Board

INFORMATION & COMMUNICATION TECHNOLOGY (ICT) ACCEPTABLE USAGE POLICY AND PROCEDURES

Document ref No.	CMETB 2017/09	Document initiated by	CMETB
Revision number	002	Document drafted by	IT Dept & FN
Document reviewed by	Senior Management	Document adopted by	CMETB
Date Document adopted	20 September 2018	Date Document implemented	20 September 2018
Assigned review period	3 Years or sooner	Responsibility for implementation	CE/Directors / Senior Management / IT Department
Responsibility for review	IT DEPT	Next review date	3 years after implementation
Original issued by	FN	Date of withdrawal of obsolete document	20.09.18

Amendment history			
Date	Revision level	Details of amendment	Approval signature
20.09.18	1	GDPR update	Fiona Nugent

This policy and procedure is being adopted and implemented on a pro-tem basis, pending the finalising of a national ICT Acceptable Usage Policy

Table of Contents

1. Scope

This policy applies to any person authorised to have access to Cavan Monaghan Education and Training Board (CMETB) information systems. This includes but is not limited to CMETB employees, contractors to CMETB and consultants engaged by CMETB hereafter collectively referred to as users for the purpose of this policy.

This policy applies to all electronic communications systems provided by CMETB including, but not limited to internet, intranet, e-mail, social media accounts, personal computers and laptops, digital cameras, PDA's (personal digital assistants) Telecommunication systems and devices. It is the responsibility of both management and staff of CMETB to ensure that all such tools are used in accordance with this policy.

All users are expected to use common sense and to conduct themselves in a manner that is appropriate to the execution of duties in the workplace. Breaches of this policy may result in personal liability of users and/or vicarious liability on behalf of CMETB under many enactments including, but not limited to the following:

- Employment Equality Acts, 1998
- Equal Status Act, 2000 and 2012
- Data Protection Acts, 1988 and 2003
- Freedom of Information Act 2014
- General Data Protection Regulations GDPR
- The Education and Training Boards Act, 2013
- The Companies Acts 1963 - 2001
- Copyright and Related Rights Act 2000, 2004 and 2007
- Child Trafficking and Pornography Act 1990 1998 and 2004

Other documentation that is relevant to this policy includes ***CMETB*** policies on:

- Social Media
- Data Protection
- Mobile Phone
- Grievance Procedure
- Discipline Procedures
- Dignity and Respect at Work
- Equality and Diversity

- Harassment and Sexual Harassment Prevention
- Bullying in the workplace Prevention
- Protected Disclosures
- Bring Your Own Device (BYOD) (in development)

2. General Computer Usage Regulations and Guidelines

2.1 Contents

All electronic content created or received using equipment or services provided by CMETB will be regarded as the property of CMETB.

2.2 Equipment and Resources

All equipment provided by CMETB for use by staff remains the property of CMETB. Employees must not remove any such equipment including but not limited to computers, laptops, mobile telephones, etc. from the CMETB's premises without prior authorisation from the line manager. If equipment is removed it must be kept in a secure environment by the user.

It is the user's responsibility to be informed of the correct operating procedures for the computer resources or products used. A user who is uncertain as to the correct procedure in any situation should obtain clarification before proceeding.

Users must not engage in conduct that interferes with other's use of shared computing resources and/or the activities of other users.

2.3 Security and Passwords

Users must not utilise any other person's access rights or attempt to gain access to resources or data. In exceptional circumstances where access is required, it must be requested in writing by the Director/Principal/Co-ordinator/Head of Department. to the Head of I.C.T. Users must not attempt to bypass or probe any security mechanisms governing access to the computer systems.

No staff member may misrepresent himself / herself as another individual. This includes using another staff member's username and password.

Passwords must remain confidential to each user and must not be relayed to any other person. The IT Department may provide the option to alter any passwords as necessary. Passwords should be changed on a regular basis (42 days for Microsoft 365 network) and should be of sufficient strength to deter

guessing or cracking. It is recommended that passwords should be a minimum of 8 characters and include a mixture of letters (upper and lower case) and numbers. Each user carries sole responsibility for security access to his/her computer, laptop or any other electronic device.

Each user must shut down his/her own computer on completion of work, and switch off all other computer equipment. In order to protect sensitive information, users should lock and password protect their PC when they are absent from their desks. Users who use devices off-site must ensure regular connection to the ETB network in order to keep the device updated.

2.4 Software Ownership

All software which is provided by CMETB to a user is licensed and owned by the CMETB and may not be downloaded, stored elsewhere or transferred to another individual by any employee of CMETB.

Under no circumstances should software be downloaded from the Internet or installed from any other source and used on the CMETB's machines without the prior permission of the IT Department/Head of IT. Any breach of these requirements may result in disciplinary action.

2.5 Software Applications (APPS)

Only Apps which are verified and authorised by the IT Department must be used by CMETB users. Users are prohibited from entering enter personal data relating to CMETB staff and/or students/learners into such Apps without prior authorisation.

2.6 Confidentiality

Users must maintain confidentiality while carrying out their duties and while on CMETB business. Users must ensure that callers to offices are unable to view personal/sensitive information displayed on computer monitors.

Users must not register with an electronic service over the internet without prior consultation with the IT Department/Head of IT, to avoid release of confidential ETB information to third parties and to avoid interference with the communication systems.

2.7 Privacy

It should be understood that CMETB does not provide users with a guarantee of, or to the right to privacy or confidentiality in connection with the use of any

technology and users should have no expectation of privacy in the use of CMETB IT resources.

2.8 Monitoring Policy

CMETB reserves the right and intent to monitor e-mail content and Internet usage to ensure technology is being used properly and to protect CMETB and its employees from liability under equality, data protection, pornography and copyright legislation. This does not constitute infringement of any individual rights to personal privacy under the Data Protection legislation.

Monitoring may be carried out on all Electronic Data including all Web site, Desktop, Laptop and Server content. This list is not exhaustive. Monitoring developments may change over time. In addition, CMETB will monitor all PC's for inappropriate images and content.

2.9 Legal Implications of Storing Electronic Data

All information held in electronic format is subject to legislative requirements, as is information held in paper format. These requirements include but are not exclusive to Copyright, Data Protection and Freedom of Information Legislation and the liabilities which may result from breaches of such legislation.

Personal information should contain only information relevant to the individual and to the purpose for which it is being stored. Personal Data obtained and stored on CMETB systems or devices must not be used for any other purpose. This data must be maintained in an accurate format and must be altered if the user/Board becomes aware of inaccuracies subject to authorisation by line management.

It is an offence to alter or falsify documents in an electronic format or paper / hard copy format. Care must be taken when forwarding or sending information which has been received from a third party or which is specific to another organisation.

Employees should be aware that merely deleting information may not remove it from the system and deleted material may still be reviewed by the employer and / or disclosed to third parties.

2.10 Material of obscene or offensive nature

Users are subject to all legislation regulating the use of CMETB's IT/ Communications resources. Users must not store, download, upload, circulate or otherwise distribute material containing:

- Any derogatory comment regarding gender, material status, family status, sexual orientation, religious or political belief, age, disability, race or membership of the travelling community or other categories pursuant to applicable law.
- Any material of a pornographic nature.
- Any material of a paedophilic nature.
- Material containing offensive or foul language.
- Any content prohibited by law.

If an employee receives any offensive, unpleasant, harassing or intimidating messages via e-mail or other computer sources the employee should bring it to the attention of their line manager, the Head of IT or Head of HR;

2.11 Virus Protection

Viruses can enter an organisation a number of different ways:

- Unscanned digital storage media (e.g. CDs, DVDs, floppy disks, USB memory sticks) being brought into the organisation.
- E-mails or attachments
- Downloaded data from the Internet.

Individuals using electronic information must be familiar with and comply with CMETB's procedures governing usage of USB's, SD Cards, CD's and other software. It is the personal responsibility of each individual to take precautions to ensure that viruses are not introduced into any CMETB resources or system with which they come into contact.

No computer user may interfere with or disable the Anti-Virus software installed on their desktop PC. Any virus, virus error messages or security incidents must be reported promptly on CMETB's Helpdesk portal https://cavanmonaghanetb.freshdesk.com/helpdesk

Do not forward a virus warning to anybody else.

Such warnings are usually hoaxes and are designed to persuade users to delete systems files on their PC; forwarding such a hoax could make CMETB liable for damage to computer systems outside the CMETB.

3. E-Mail

Employees have a CMETB e-mail account to facilitate the sending and receiving of business messages between staff and between CMETB and its clients and suppliers. All communications should be carried out using the user's CMETB email address only. While email brings many benefits to CMETB in terms of its communications internally and externally, it also brings risks to the organisation, particularly where employees use it outside of their CMETB roles.

Every employee has a responsibility to maintain CMETB's image, to use electronic resources in a productive manner and to avoid placing CMETB at risk for legal liability based on their use. It should be remembered that the contents of e-mail are considered as official records for the purpose of legislation such as Freedom of Information Act, National Archives Act, and GDPR.

3.1 Risks Associated with E-Mails

- Messages can carry viruses that may be seriously damaging to CMETB's systems

- E-Mail attachments may belong to others and there may be copyright implications in sending or receiving them without permission.

- It has become increasingly easy for messages to go to persons other than the intended recipient and if confidential or commercially sensitive, this could be breaching CMETB's security and confidentiality.

- E-mail is speedy and, as such, messages written in haste or written carelessly are sent instantly and without the opportunity to check or rephrase. This could give rise to legal liability on the part of CMETB.

- An e-mail message may legally bind CMETB contractually in certain instances without the proper authority being obtained internally.

- E-mails should be regarded as potentially public information which carries a heightened risk of legal liability for the sender, the recipient and the organisations for which they work.

3.2 Rules for E-Mail Use

The content of any e-mail must be in a similar style to that of any written communication such as a letter or report as they have the same legal standing. It is important that e-mails are treated in the same manner as any other written form of communication in terms of punctuation, accuracy, brevity and confidentiality. Similarly, any written, stored or forwarded and disseminated information must adhere to the guidelines within the Data Protection and the Employment Equality legislation and in accordance with the equality policy of CMETB.

In order to avoid or reduce the risks inherent in the use of e-mail within CMETB the following rules must be complied with:

- The CMETB's email disclaimer or a link to same must appear at the end of every e-mail sent from your CMETB's address to an external address.
- The CMETB's/school/centre name is included in the address of all staff members and is visible to all mail recipients. This reflects on the image and reputation of the organisation, therefore, e-mail messages must be appropriate and professional.
- Correct spelling and punctuation should be maintained in all communications.
- Corporate e-mail is provided for business purposes.
- CMETB emails must not be forwarded or redirected to any personal or private email system outside the management of CMETB IT.
- Occasional and reasonable personal use of e-mail is permitted provided that this does not interfere with the performance, work duties, responsibilities and customer service of CMETB. It does not support any business other than CMETB and otherwise complies with this policy.
- An e-mail should be regarded as a written formal letter, the recipients of which may be much more numerous than the sender intended. Therefore, any defamatory or careless remarks can have serious consequences, as can

any indirect innuendo. The use of indecent, obscene, sexist, racist, harassing or other appropriate remarks whether in written form, cartoon form or otherwise is forbidden.

- E-mails must not contain matters which may discriminate on grounds of gender, marital status, family status, age, race, religion, sexual orientation, disability or membership of the Traveller community.
- E-Mails must not contain any inappropriate or lewd content or content likely to cause offence.
- Distribution lists may only be used in connection with CMETB business.
- Documents prepared internally for the public or for clients may be attached via the e-mail. However, excerpts from reports other than our own may be in breach of copyright and the author's consent should be obtained particularly where the excerpt is taken out of its original context. Information received from a customer should not be released to another customer without prior consent of the original sender. If in doubt consult your manager.
- Do not subscribe to electronic services or other contracts on behalf of CMETB unless you have express approval to do so from your line manager and/or the IT Department.
- If you receive any offensive, unpleasant, discriminatory, harassing or intimidating messages via the e-mail system you must immediately inform your manager or the Head of HR.
- Chain mails or unsuitable information must not be forwarded internally or externally.
- CMETB reserves and intends to exercise the right to review, audit, intercept, access and disclose all messages created, received or sent over the electronic mail system for any purpose or where it deems necessary.
- Notwithstanding CMETB's right to retrieve and read any electronic mail messages, such messages should be treated as confidential by other employees and accessed only by the intended recipient. Employees are not authorised to retrieve or read any e-mail messages that are not sent to them. However, the confidentiality of any message should not be assumed. Even when a message is erased it is still possible to retrieve and read that message.
- When a user registers with a site or a service in the name of CMETB the resulting spamming of information may tie up the communications system. Users must not register with an electronic service or website without prior permission from their Line Manager and from the Head of IT, to avoid the release of confidential CMETB information to third parties and to avoid interference with the communications systems.

- Users should take the time to review each email before sending to ensure the message is clear and is relaying the right tone (Try reading it out loud). It may be useful to ask yourself are you happy that the content of the email could be displayed on a public notice board if not consider rephrasing or using other means of communication.
- Particular care should be taken when sending attachments. Users should open and check each attachment before sending, in order to ensure that the correct file has been attached.
- Users should avoid sending email text in capitals. IF YOU WRITE IN CAPITALS IT SEEMS AS IF YOU ARE SHOUTING. This can be frustrating and may trigger an unwanted response from the recipient.
- 'Reply All' should be used only if it is necessary for the message to be seen by each person who received the original message. In most cases, replying to the Sender alone is sufficient.
- In most circumstances, emails are sent and received during normal business hours. Only in exceptional circumstances should emails be sent for delivery after 7:00 pm at night or at the weekend. CMETB does not expect staff to read or reply to emails received after 7.00 pm at night or at the weekend.
- CMETB does not expect staff who are absent on leave to read or reply to emails received on their CMETB staff email address. This also applies to staff who have remote access to their CMETB work email address.
- CMETB email users may choose to have their emails forwarded to another CMETB staff members' CMETB mailbox, however, CMETB emails should not be forwarded to any other personal or private email system outside the management of CMETB IT. An example of a personal or private email system is but is not limited to Gmail, Hotmail, Yahoo, AOL, Eircom, Outlook Live etc.
- CMETB staff email users on an extended absence should create an Out Of Office message, which should include the contact information for another staff member who can respond while the absent member is away from the office.
- In the event the absent staff member has not setup the Out Of Office, CMETB IT, on the instruction of senior management, will either put an out of office email on or authorise another staff member to check email or redirect emails to an authorised CMETB staff member's mailbox.
- If the message is important, users should obtain confirmation that the intended recipient(s) received your email by using the "Request a Read Receipt" option on the Tools menu. However, this function should not be used to automatically request a receipt for every email sent, it should be used only as required.

- Messages should be regularly reviewed and those that have been actioned and are no longer needed should be deleted, in order to ensure that disk space is managed efficiently.
- Users should be aware of the risk of viruses being sent in email messages or attachments. Users should be vigilant for unsolicited or unexpected emails and never open attachments or click on links contained in emails from addresses or people they do not recognise.

4. The Internet/Intranet

CMETB provide a managed network across all its schools and centres. Access to the Internet/Intranet/network is provided to staff as necessary solely for the purpose of conducting CMETB's business. All information and uploaded content on the intranet is the property of the CMETB.

4.1 Rules for Internet use

- CMETB Internet connections are intended for activities that either support CMETB's business or the professional development of employees.
- Internet usage may be monitored on a systematic basis and as deemed necessary by the IT Department.
- Unauthorised downloading of any software programmes or other material is forbidden.
- It is a disciplinary offence to access, download, save, circulate or transmit any racist, defamatory or other inappropriate materials or materials that may discriminate on the grounds of gender, marital status, family status, age, race, religion, sexual orientation, disability or membership of the Traveller community. This rule will be strictly enforced and is viewed very seriously with potential criminal liabilities arising therefrom.
- It is a disciplinary offence to access, download, save, circulate or transmit any indecent, obscene, child pornographic or adult pornographic material.
- If an employee is downloading pornographic images within view of a colleague or forwarding those images to a colleague, this may result in harassment or sexual harassment by offended parties. Such incidents should be reported to CMETB. Apart from any potential offence caused and the inappropriateness of such activity, CMETB may be vicariously liable for any claims arising from such behaviour.
- Because of the serious criminal implications of accessing child pornography, any employee found to be accessing such information may be summarily dismissed and the matter referred to An Garda Síochána. Furthermore,

should an employee be prosecuted under the Child Trafficking and Pornography Act, 1998, by engaging in such activities outside the remit of the workplace, CMETB may find it fitting to invoke disciplinary action.

- The Internet must not be used to pay for, advertise, participate in or otherwise support unauthorised or illegal activities.
- The Internet must not be used to provide lists or information about the organisation to others and/or to send classified information without prior written approval.

4.2 Rules for Network Use

- Employees may not tamper with any network equipment/cabling unless instructed by a member of the IT department.
- Employees are strictly prohibited from installing/connecting any additional network equipment E.G. wireless access points, wireless routers, 3G dongles without prior approval from the IT department.

5. Laptops and Remote Devices supplied by CMETB

The rules applying to use of the Internet and email messaging systems apply also to any laptops, tablets, mobile phones or other electronic devices in use by staff members and supplied by CMETB.

All devices should be password and/or PIN protected to prevent unauthorised use of the device and unauthorised access to information held on the device.

Personal, sensitive or confidential data should not be stored on laptops or other portable devices, however where this is unavoidable, the device should be equipped with encryption software. Anti-virus/Anti-spyware/Firewall software must be installed and kept up-to-date on all portable devices. All personal data stored on CMETB mobile devices must be protected by encryption software.

Authorisation must be obtained from the Line Manager to remove such equipment/devices from ETB premises. All such equipment will be subject to the same monitoring procedure as that which is retained on-site.

6. Bring your own device (BYOD)

Employees may use their own mobile devices to access CMETB resources such as email, calendar, intranet, contacts, and documents. Access to CMETB

networks is granted on the same basis as that of employees using CMETB owned devices and is subject to the same security measures being employed.

In order to prevent unauthorised access all devices must:

- Be password/PIN code protected using the features of the device
- Have encryption enabled (see Appendix 2 for details on enabling encryption on IOS and Android devices)
- Lock itself with a password or PIN if its idle for five minutes
- Use a strong password and 2 factor authentication to access CMETB systems
- Have Anti-virus/Anti-spyware/Firewall software installed and kept up-to-date.

Rooted (Android) or jailbroken (IOS) devices are strictly forbidden from accessing CMETB systems

Personal data relating to CMETB staff and students should not be stored on employee's own mobile devices, it must be stored directly onto the CMETB Microsoft 365 network (e.g. OneDrive, OneNote, SharePoint), however where this is unavoidable it must be protected by encryption software.

Employees using their own devices to access CMETB resources must report the lost or theft of such devices to their line manager and the IT Department without delay.

The employee's device may be remotely wiped by the IT Department if:

- The device is lost or stolen
- The Employee terminates his or her employment with CMETB
- IT detects a data or policy breach, a virus or similar threat to the security of CMETB's data and systems

In the event that CMETB must wipe a device, every precaution will be taken to prevent the employee's personal data from being lost but it is the employee's responsibility to take additional precautions, such as backing up email, contacts and documents.

7. Telephone Usage

Access to telephones is intended for CMETB purposes only. While reasonable making and taking personal calls is not strictly prohibited, staff are encouraged to keep this to a minimum level. CMETB reserves the right to monitor the use of the telephone system.

Some mobile phones are provided to staff members for CMETB business. Personal calls from such phones are permitted but the calls must be paid for by

the staff member. For more specific information see CMETB's Mobile Phone Policy.

During office hours, the taking and/or making of calls on personal mobiles is not strictly prohibited however, staff are encouraged to keep such calls to a minimum. The making and receiving of personal call or texts, particularly during the course of classes or meetings, is deemed inappropriate.

8. Other Electronic Tools

Other electronic equipment (e.g. fax machines, photocopiers etc.) remain the property of CMETB and as such must be treated with care and used only for CMETB purposes. Abuse of equipment for personal use or gain may result in the use of the disciplinary procedures and in disciplinary action.

9. Plagiarism

Users should not plagiarise (or use as their own, without citing the original creator) content, including words or images from the Internet. Users should not misrepresent themselves as the author or creator of something found on-line. Research conducted via the Internet should be appropriately cited, giving credit to the original author.

10. Social Media

CMETB recognises the presence and value of social media tools which can facilitate communication, learning and collaboration. When using these tools, users are expected to communicate with the same appropriate and professional conduct online as offline.

Users should consider rules governing copyright, intellectual property and confidentiality before posting to social media.

Users should be mindful of their privacy settings and postings on personal social platforms. Employees should note that the use of social media in a work setting is subject to the same guidelines and rules as previously outlined in this policy. For more specific information see CMETB's Social Media Policy.

11. Removable Media

No non-CMETB approved removable media such as CD, DVD, USB drive or SD cards etc. that contain data or files may be used without consulting with the IT Department. Removable media must not be used to store personal data of CMETB staff or students/learners.

12. Encryption

All personal data stored on CMETB mobile devices must be protected by encryption software. It is the responsibility of the staff member to ensure that the data is encrypted and the encryption software is up to date. This responsibility includes data stored on personal devices.

Only encryption software recommended by CMETB should be used. For guidance on enabling encryption on mobile devices see Appendix 2.

13. Infringements of Policy

Failure to comply with the policy and guidelines outlined above may result in:

- The withdrawal of e-mail and Internet facilities from the Section, Staff or members involved
- Initiation of disciplinary procedures and disciplinary action, up and to including dismissal.
- Serious breaches of the policy may result in initiation of criminal or civil proceedings.

14. Training and Support

14.1. Training

Training and support will be provided to users as and when required in order to assist in the appropriate use of ICT resources across CMETB services.

14.2. CMETB IT Helpdesk

The IT Department have a helpdesk portal for all users. This portal helps to streamline the support process and make it easier for all users to track the status of their support requests.

- Users can access the Helpdesk portal in two ways.
    - The web-link in the user's Internet Explorer favourite's list
    - Via the CMETB Website www.cmetb.ie
- By selecting the Helpdesk web-link the user will be then presented with the login page where the user will input their CMETB username ***(full-name no spaces)*** and current CMETB password to gain access to the Helpdesk portal.
- Once successfully authenticated the CMETB Helpdesk portal will be presented to the user where they can continue to create a ticket about the issue(s) by selecting **New Support Ticket** button.
- The user will continue to fill in the support request form by filling in the mandatory fields and selecting the appropriate pre-populated options.
- Once the ticket is submitted a support agent will be assigned the ticket. The affected user will get notifications on any updates of the ticket in their portal and also directly to their CMETB email.
- **NB** It is recommended that the affected user continues to use the CMETB Helpdesk portal as the only communication mechanism for all Helpdesk queries.**

15. Implementation and Review

The Chief Executive of CMETB and delegated Officers (Directors, Head of IT, Principals, Centre Managers, Programme Co-ordinators, APOs and Section Heads) are responsible for implementing this policy. However all staff members who have access to CMETB ICT systems are individually responsible for compliance with this policy. CMETB will provide support, advice and training to all staff concerned as and when deemed necessary.

This policy will be reviewed regularly and/or in light of any legislative or other relevant indications.

This Policy was adopted by Cavan and Monaghan Education and Training Board at the meeting of the Board on 20 September 2018.

Appendix 1

AUTHORISATION FORM EMAIL AND IT SYSTEM ACCESS

Part A

The following person is to be set up with an email address:

NAME _____

CENTRE NAME _____

DEPARTMENT(s) _____

Does the user require an email address? YES ☐ NO ☐

Please add the above named to the following email distribution lists:

_____

_____

_____

Please give the above named access to the following Applications/Folders:

_____

_____

_____

Signed: _____ Date: _____

HEAD OF DEPARTMENT

To be signed by employee/volunteer/work placement student:

I have received and read a copy of CMETB ICT Acceptable Usage Policy and undertake to use the above email address and IT Systems/Folders for authorised use only, as outlined in the Policy.

Signed: _____ Date: _____

Authorised by: _____ Date: _____

APO/PRINCIPAL/DIRECTOR/MANAGER

Part B

Please remove access to email address and Applications/Folders for the above named

w.e.f. _____

Signed: _____ Date: _____
HEAD OF DEPARTMENT

Authorised by: _____ Date: _____
APO/PRINCIPAL/DIRECTOR/MANAGER

NB - This form completed and duly authorised should be given to IT personnel.
IT personnel will not set up/remove email addresses or give access/withdraw access to IT Systems without this Authorisation Form being completed and authorised in advance.

For IT Personnel Use only –
Email address set up / access to Applications/Folders given on
_____(date)

Email address removed / access to Applications/Folders withdrawn on
_____ (date)

Appendix 2

How to encrypt and password protect your Android phone

1. To setup a PIN on your phone under Settings > Security > Screen Lock and set your PIN.
2. To set up encryption, plug your phone into a power source. The process can take an hour or more depending on how much data requires encrypting.
3. Ensure that you have backed-up all your important data.
4. Go to Settings -> Lock Screen -> Screen Lock -> [enter current password] -> Password and create a password that is at least 4 characters long, and contains at least 1 number. Note there is a limit of 16 characters. If you do not perform this step first, you will be sent back to do it when you start to encrypt your device
5. Go to Settings -> System -> Security -> Encrypt device
6. Select "Encrypt Phone" to confirm encryption. You will be asked once more to confirm your password.
7. Once completed, you need to enter your master password each time you reboot your phone

How to encrypt and password protect your iPhone

1. Go to the Settings on your phone.
2. Go to Touch ID & Passcode.
3. Select the Turn Passcode On option if it is not already. From there, you will be able to set either a strong six-digit or longer numerical passcode, or alphanumeric password.
4. Set a strong passcode. If you enter a code like "123456" it will warn you that it is easy to guess.
   At this screen, selecting Passcode options will allow you set a longer numerical passcode by choosing Custom Numeric Code. This offers the benefit of only giving you numbers to press on the lock screen.
   You can also set a Custom Alphanumeric Code, which significantly improves your device's security. According to Apple, setting a six-digit alphanumeric passcode with a combination of lower-case letters and numbers would take about five years to break if every combination was tried.
5. Once your passcode is set, you will return back to the Settings menu. Scroll down to the bottom of the page, you should see: "Data protection is enabled." That means your device is now encrypted.

The instructions above may vary depending on your device manufacturer/model. Please consult your device documentation for more information if required.

If you need technical assistance with this process please create a support request on the CMETB helpdesk at: https://cavanmonaghanetb.freshdesk.com/helpdesk