City of Dublin Education and Training Board

Encryption Policy

Document version	2
Drafted by	ETBI (ICT Group)
Responsibility for this policy in City of Dublin ETB	Director OSD and Head of IT
Reviewed by Senior Leadership Team (SLT)	12 October 2021
Approved by Chief Executive	12 October 2021
Noted by Board	21 October 2021
To be reviewed	1 year from date of approval by CE

Contents

1 Introduction

1.1 Purpose of this Document

The Encryption policy is defined in the City of Dublin ETB ICT Framework Policy and should be read in conjunction with all other ICT policies to ensure that required security standards are adhered to, the purpose of this policy is to protect the confidentiality, integrity, and availability of City of Dublin ETB information, records and data by applying appropriate levels of cryptographic control. The policy will serve to identify the business requirements for when encryption must be used and the standards that are to be implemented. Consideration must also be given to the rights of third parties to receive access to the unencrypted data, *e.g.* An Garda Síochana.

1.2 Scope and Constraints

This policy applies to all users referred to in the definitions section, it includes the use of all City of Dublin ETB technology infrastructure, user BYOD devices and removable storage. This policy is effective as of the issue date and does not expire unless superseded by another policy.

1.3 Definitions

A full range of definitions is available in the ICT Frameworks Policy

1.4 Policy Review, Approval and Continuous Improvement

In line with best practice, this policy has been approved by senior management, along with its commitment to continually improve the protection of all City of Dublin ETB information assets and the protection of personal data where City of Dublin ETB is a controller or processor.

This document will be reviewed at least annually by senior management, to ensure alignment to appropriate risk management requirements and best practice for the management of ICT devices within City of Dublin ETB.

2 Encryption Policy

2.1 ICT Technical Standards

1. Where encryption is used, only industry recommended standards such as Microsoft Bitlocker must be employed. It is not acceptable to deploy a bespoke encryption methodology.

   The encryption procedures in place in City of Dublin ETB must be compliant with relevant legal requirements**.**

2. Any proposed deployment using PKI and/or certificate-based authentication should involve **IT Department**. Specifically, the following policy applies:

    a. Procedures must be established for registration, generation, distribution, recovery, renewal, revoking and destroying of digital certificates associated with users.
    b. The private keys for user certificates used for authentication and signatures should be stored on encrypted cards or devices.
    c. Systems that use mechanisms based on digital certificates for identification and authentication for the user access will confirm:
        i. Validity and expiration of the certificates;
        ii. Ensure they lead to a trusted root and that they have not been revoked.
    d. The period of the validity of the personal digital certificates or private keys must be established by your local information security officer, in line with local laws;

3. All User devices must be encrypted before being used to process or store Corporate Data.

2.2 User Responsibilities

1. When processing Corporate Data, the following standards of care are expected:
    a. All Corporate Data should be processed using only approved applications and protocols within the ICT framework Policy
    b. All Sensitive Data should be processed as above, but if being transmitted requires an addition level of protection achieved by following City of Dublin ETB's IT Department guidance

    For further guidance please refer to City of Dublin ETB's Data Processing Policy.
2. Where a third-party requires a specific practice to transfer data, approval from the IT Department is required before initiating the process.
3. Where password-based encryption is used, it is extremely unsafe to send the details along with or in subsequent emails; the IT Department requires e.g. phone call, SMS or other as a means to communicate this highly privileged information.
4. All encryption key/passwords should be stored securely to facilitate file access and data recovery. Storage of this information must never be in plain text documents or hard copy
5. Any encrypted files remain the property of City of Dublin ETB. Upon request, all passwords, encryption keys, and any ancillary information that would facilitate access to the encrypted files must be made available to City of Dublin ETB.
6. Any suspicious activity must be promptly reported to City of Dublin ETB's IT Department.
7. For the avoidance of doubt, where questions remain as to what constitutes "approved applications and protocols", contact City of Dublin ETB's IT Department for full clarification.
8. Guidance on encrypting a personal mobile device is included in Appendix A.

3 Enforcement

Individuals found to be in breach of this policy may be subject to disciplinary action, up to and including dismissal. Should an investigation regarding compliance with this policy determine that there is a case to answer by a User, the matter will be referred to the appropriate stage of the relevant disciplinary procedure as appropriate to that User.

4 Appendix A

How to encrypt and password protect an Android phone

1. To setup a PIN on an Android phone navigate to Settings > Security > Screen Lock and set a PIN.
2. To set up encryption, plug the phone into a power source. The process can take an hour or more depending on how much data requires encrypting.
3. Ensure to back-up all 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. This step will need to be completed in order to start encrypting the device.
5. Go to Settings -> System -> Security -> Encrypt device
6. Select "Encrypt Phone" to confirm encryption. the device will prompt to confirm password

Once completed, the device will require a password in order to successfully boot, and on all subsequent reboots.

How to encrypt and passcode protect an iPhone

1. Go to the Settings on the phone.
2. Go to Touch ID & Passcode.
3. Select the Turn Passcode On option if it is not already. From there, set either a strong six-digit or longer numerical passcode, or alphanumeric password.
4. Set a strong passcode. If a code like "123456" is used it will warn that it is easy to guess.

- At this screen, selecting Passcode options will allows a longer numerical passcode to be set by choosing Custom Numeric Code. This offers the benefit of only giving you numbers to press on the lock screen.
- A Custom Alphanumeric Code can also be set, which significantly improves device 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 a passcode is set, it will return back to the Settings menu. Scroll down to the bottom of the page and "Data protection is enabled." should be present, That means your device is now encrypted.

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

How to encrypt and password protect a Windows 10 Mobile

Device encryption is an option that comes disable by default, but the feature can easily be enabled using the following steps:

1. While in the Start screen, swipe left to bring All apps, then search for and open the Settings app, and tap on System.

2. Next, tap on Device encryption.

3. Finally, make sure to slide the Device encryption pill switch to the On position to enable the feature.

4. Important Note: A password PIN must be in place to enable the feature if the mobile device doesn't have one when trying to enable Device encryption, the user will be automatically redirected to the Sign-in options settings page to create a PIN. Then tap the Add button, under the PIN section, and follow the on-screen wizard to create a new PIN. After the PIN password is created, go back to Device encryption settings to verify that the feature has been enabled.

5. While the feature should work as expected, Windows Phone 8.1 used to display an "encrypted" label in the phone storage settings, and Windows 10 Mobile doesn't provide such visual confirmation in the storage settings. The only way to verify the device is being encrypted is by making sure the "Device encryption" is turned on in the Settings app.

6. It's important to point out that while encryption is enabled on a mobile device, the operating system and data stored in the local storage will be encrypted, but device encryption will not encrypt data that is stored on an SD card. As such, it's highly recommended that sensitive data is not stored on removable storage, as anyone could easily remove the storage and have unrestricted access to that data from any computer.

Furthermore, users need to be careful when to choose to enable this feature, as it's possible that encrypting a device may cause some issues, such as problems with emails not synchronizing with the user’s mobile phone.