CBS Secondary School, Dungarvan.

Encryption Policy

As stated in our mission statement, Dungarvan CBS Secondary School is concerned with the overall well-being of the student that cares for the spiritual, intellectual, social, physical and emotional well-being of each student.

Purpose

The purpose of this policy is to define the acceptable use and management of encryption software and hardware throughout CBS Secondary School, Dungarvan.

Principles of Encryption

Where possible all confidential and restricted information must be stored securely on the school server with restricted access. Where it has been deemed necessary to store confidential or restricted information on any device other than a school network server the information must be encrypted.

All confidential and restricted information transmitted via email to an email address outside of the dungarvancbs.com domain (i.e. one that does not end in "@dungarvancbs.com") must be encrypted.

All passwords used as part of the process to encrypt/decrypt information must meet the requirements of Dungarvan CBS Encryption Policy.

Servers

Confidential and restricted information stored on shared Dungarvan CBS network servers which are situated in physically are protected by the use of strict access controls and encryption software.

Desktop Computers

Desktop computers which for business, geographic or technical reasons need to permanently store confidential or restricted information locally on the computer's hard drive must be fully encrypted with full disk encryption.

All Dungarvan CBS laptop computer devices that stores confidential and restricted information must have Dungarvan CBS approved encryption software installed prior to their use. In addition, to encryption software, the laptop must be password protected and have up-to-date anti-virus software installed.

The preferred method of encryption for laptop computers, mobile computer devices and smart devices is whole disk encryption. Mobile computer devices and smart devices which are not capable of whole disk encryption must use file/folder level encryption to encrypt all confidential and restricted information stored on the device.

Laptop, mobile computer devices and smart devices must not be used for the long-term storage of confidential and restricted information.

Removable Storage Devices

All confidential and restricted information stored on removable storage devices must be encrypted. In addition to being encrypted, removable storage devices must be stored in a locked cabinet or drawer when not in use.

Removable storage devices except those used for backup purposes must not be used for the long-term storage of confidential and restricted information.

The preferred method of encryption for removable storage devices is whole disk/device encryption. Where whole disk encryption is not possible, then file/folder level encryption must be used to encrypt all confidential and restricted information stored on the removal storage device.

USB Memory Sticks

Confidential and restricted information may only be stored on encrypted USB memory sticks.

Encrypted USB memory sticks must only be used on an exceptional basis where it is essential to store or temporarily transfer confidential or restricted information. They must not be used for the long term storage of confidential or restricted information, which must where possible be stored on a secure Dungarvan CBS network server.

Confidential and restricted information stored on the encrypted USB memory stick must not be transferred to any internal (except a secure Dungarvan CBS network server) or external system in an unencrypted form.

Transmission Security

All confidential and restricted information transmitted around existing wireless networks must be encrypted using WEP (Wired Equivalent Privacy) or better. All new wireless networks installations must be encrypted using WPA (Wi-Fi Protected Access) or better.

Roles & Responsibilities

IT Support is responsible for:

- The selection and procurement of all encryption facilities used within Dungarvan CBS.
- The provision, deployment and management of encryption facilities within Dungarvan CBS.
- The provision of training, advice and guidance on the use of encryption facilities within Dungarvan CBS.

Information Owners

Information owners are responsible for:

- The implementation of this policy and all other relevant policies within Dungarvan CBS.
- Making sure adequate procedures are implemented within Dungarvan CBS, so as to ensure all staff, third parties and others that report to them are made aware of, and are instructed to comply with this policy and all other relevant policies;

Users

Each user of Dungarvan CBS IT resources is responsible for:

- Complying with the terms of this policy and all other relevant HSE policies, procedures, regulations and applicable legislation.
- Respecting and protecting the privacy and confidentiality of the information they process at all times.
- Ensuring all encryption passwords assigned to them are kept confidential at all times and not shared with others;
- Ensuring encryption passwords used to access encrypted devices are not written down on the encrypted device or stored with or near the encrypted device;
- Reporting all misuse and breaches of this policy to management.

Full Disk Encryption Certifications:

FIPS 140-2 level 1

Algorithms & Standards:

AES 256 bit AES 128 bit
SHA 256 bit
RSA 1024 bit
Triple DES 112 bit
Blowfish 128 bit

Encryption Key Management

Key management must be fully automated.
Private keys must be kept confidential.
Keys in transit and storage must be encrypted.

Enforcement

Dungarvan CBS reserves the right to take such action as it deems appropriate against individuals who breach the conditions of this policy. Dungarvan CBS staff, students, contractors, sub-contractors or agency staff who breach this policy may be subject to disciplinary action, including suspension and dismissal as provided for in Dungarvan CBS disciplinary procedures.*
Dungarvan CBS will refer any use of its IT resources for illegal activities to the Gardaí.

Policy Review:

This policy will be reviewed as necessary and particularly to comply with any relevant legislative changes.

Proposed by: _____ Chairperson _____

Seconded by: _____ Date: _____