Laptop Encryption Service – FAQ

Q: What is laptop encryption, and what does it do?

A: Laptop encryption (more specifically, whole disk encryption) is a technology that protects the contents of your laptop from unauthorized access by converting it into unreadable code that cannot be deciphered easily. It is a much stronger level of protection than typical security features, such as logging into an operating system with your password or protecting individual files with passwords.

Q: How does encryption work?

A: There are many types of encryption but the basic concept is to encode information (data) so that only those with the right "key" can decode and use it. Your "key" is the password you enter when you turn on your laptop.

Q: How much does it cost to encrypt my laptop?

A: For any DCU purchased laptop, encryption is provided at no additional charge.

Q: I have a desktop computer that stores confidential data listed above. Can I have it encrypted?

A: This project will focus on encrypting laptops, but some high-risk workstations may also be encrypted in the future

Q: How long does it take to encrypt my hard drive?

A: It takes about 20 minutes to install the encryption software, and then between 4 and 10 hours to finish the encryption, during which time you can use your computer normally. After the initial encryption is complete, the encryption should not disturb you while you work.

Q: Will my computer act differently after it has been encrypted?

A: The only difference will be that you have to enter a password into your computer when you first turn it on. This separate password ensures only you can access your encrypted data. You will assign a separate password for this purpose and then login into windows as normal

Q: Will my computer run slower once it is encrypted?

A: Occasionally there is a minute reduction in computer speed after encryption. In general, this is unnoticeable on all but very old laptops - i.e., those more than 4 years old.

Q: Should I back up my computer before it is encrypted?

A: Yes! While we do not anticipate having any problems during the encryption process, it is always a good practice to back up your data before encrypting your laptop. If you need assistance with your backup, please contact Support.

Q: What happens if I forget my password? Will I be locked out of my data forever?

Mcafee Encryption uses a recovery token that we will record during the initial configuration. If you forget your password, you will need to contact the Service Desk, they will use the recovery token to allow you to bypass login.

Q: What if I use my own personal laptop? Does that need to be encrypted?

A: Personally-owned laptops are not in the scope of the current encryption project

Q: Will laptop encryption cause problems with any of the applications I use?

A: Encryption should cause no problems with software and should be transparent to the general usage

Q: If my laptop is encrypted, is my data totally safe?

A: If your hard drive is encrypted, the data stored on it cannot be accessed if the drive is put into another computer or if somebody boots up off a CD or other media.   Your data is still vulnerable to network attacks, password guessing, viruses, malware and other compromises.

Q: If I copy files from my encrypted laptop to an external device or file share, will the files be encrypted?

A: No. Any data that you access will be transparently unencrypted before use.

Q: Once my laptop is encrypted, can I store Restricted Information on it?

A: Yes, however since hard drive encryption still leaves data on laptops vulnerable to many other attacks, you should carefully consider the need to store Restricted Information on a laptop.

Q: If I use automated software to back up my laptop, will the backups be encrypted?

A: No. Any data accessed by applications will be transparently unencrypted before use. If the backups contain Restricted Information, then be sure to encrypt the backup media or files.

Q: Once my laptop is encrypted, do I still have to use VPN?

A: Yes. Laptop encryption encrypts the data sitting on your hard drive. VPN encrypts data traveling across the network.

Q: If I connect an external hard drive or USB drive, will it be encrypted?

A: No.

Q: How do I let other people share my laptop? How should they login?

A: For staff users we can setup additional authorized users to the Encryption login as each person needs to have their own separate login and details should never be shared.

Q: What if I forget my encryption password

If you forget your pre-boot Encryption password, you will not be able to access your laptop and the data files on the computer ie. you will not be able to get past the pre-boot login screen. The only solution to this scenario is for you to call the IS Services desk so that a member can reset your pre-boot encryption password.

This is one of the reasons why full disk Encryption is secure as without the correct pre-boot password you cannot access the laptop and its data files, so it is imperative that you remember this password.

Q: What if my windows Network Login Password Expires

After the Encryption software has been installed if your network login password expires you can change your password as normal.

Q: What if my windows Network Login Account is Locked-out

If your windows account is locked out you will be able to login with the Mcafee Encryption when you start up your laptop but you will not be able to login to Windows. Therefore you will have to go through the normal account lockout procedure before being able to access your data once more.

Q: What are the minimum hardware requirements for Encryption Installation?

A: 1 GB of RAM, Minimum 5GB hard disk space

Q: What Operating Systems support Mcafee Encryption?

A: It supports the following operating systems:

Windows 7 (all 32- and 64-bit editions)   Windows XP Professional (32/64- Bit)

Apple Mac OS X10.5.8 and above (Intel-based Macs only)

Q: What if I Leaving College or would to Uninstalling Mcafee Encryption

A: As per the terms and conditions of this encryption service, if your account expires or is disabled all encryption facilities will be terminated. In the event of such termination users are obliged to contact the IS Service Desk so that the licensed Mcafee FDE software can be removed.

This is of relevance to those members of staff planning to leave College permanently. In this instance the member of staff should contact the IS Service Desk in advance to arrange for the uninstallation of the licenced Mcafee FDE software.