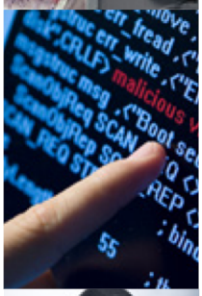
Crime prevention advice for
Data Encryption



Data is of paramount importance to any business but if it is accessed by unauthorised individuals or even criminals it could have a range of damaging implications. If your business handles confidential information it is worth considering using encryption in order to ensure that if data gets into the wrong hands, the details in this data cannot be accessed.

How does encryption work?

Encryption uses a key to encrypt data and that same key is needed to decrypt the data. The process of encryption runs the data through a formula meaning it cannot be understood by a third party. Encryption can be carried out on data that is stored but it can also be used in transferring data, i.e. via email.

Storing Data and Transferring Data

Storing data

- When storing sensitive data whether it is a backup or working data, you should always check what level of encryption is used.
- Whether it is in the cloud or a physical backup, you should know where the data is at all times.

Transferring Data

- When moving sensitive data it is important to encrypt this in case of loss.
- Transferring data electronically is preferable as even if removable devices such as memory sticks are encrypted, these can easily be lost.

Information Commissioner's Office

In the event of data being lost or stolen, you may need to notify the Information Commissioner's Office. If you have encrypted the data, the consequences may not be as severe due to you taking greater steps to ensure the data cannot be interpreted, even if it is intercepted.

It is important to remember that the level of encryption used with be determined by the sensitivity of the data you are dealing with. The implementation of this will also vary in complexity therefore you may need to consult your IT department or a specialist.