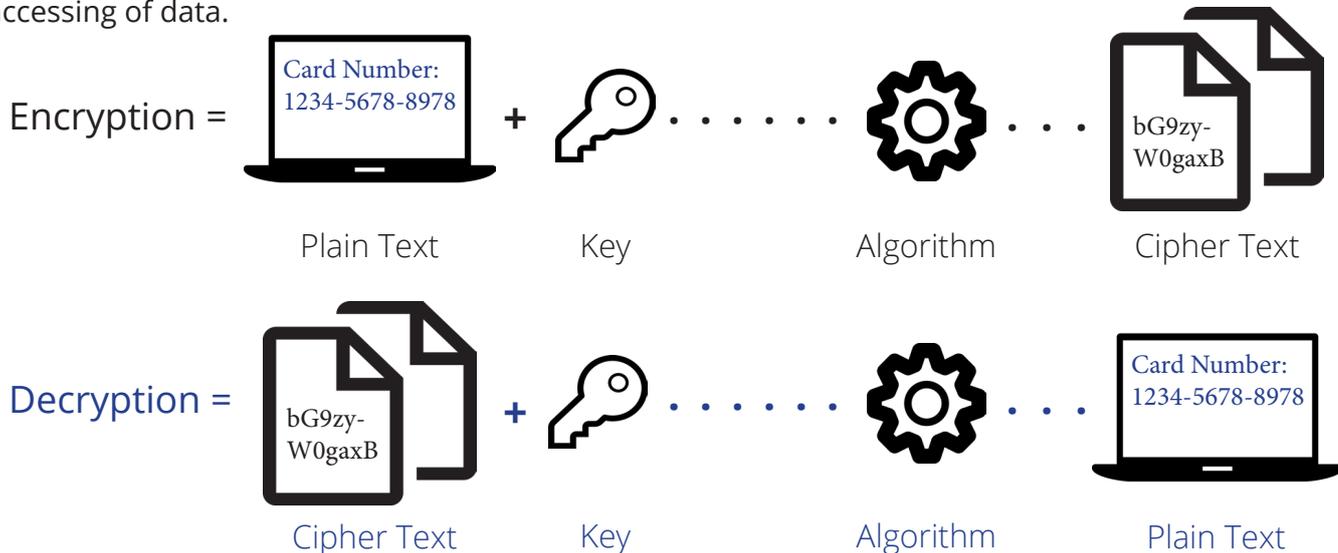## What is Encryption?

In basic terms encryption is a method of protecting data from people you don't want to see it. Encryption is a mathematical function using a secret value — the key — which encodes data so that only authorised users with access to that key can read the information.

In many cases encryption can provide an appropriate safeguard against the unauthorised or unlawful accessing of data.

Encryption =

| Plain Text | Key | Algorithm | Cipher Text |

Decryption =

| Cipher Text | Key | Algorithm | Plain Text |

Why should I use Encryption?

There are many strong arguments for using encryption as part of your Data Protection and IT Security policies and plans. Two very important reasons to implement an encryption solution relate to upcoming legislation and a change in policy from the Information Commissioners Office.

The General Data Protection Regulation (GDPR) legislation comes into effect from the 25th May 2018. There are a range of measures that organisation must do to ensure that they meet the requirements of this new law. Fines for non-compliance or a data breach are up to £16 million. The new law does state that if data is lost but is in an encrypted format then this does not constitute a data breach and action will not be taken against a company. It therefore seems sensible to encrypt sensitive data to ensure compliance and to avoid fines and regulatory action.

The Information Commissioners Office have also recently stated:

"In recent years there have been numerous incidents where personal data has been stolen, lost or subject to unauthorised access. In many of these cases, these were caused by data being inadequately protected or the devices the data was stored on being left in inappropriate places – and in some cases both. The Information Commissioner has formed the view that in future, **where such losses occur and where encryption software has not been used to protect the data, regulatory action may be pursued."**

Action will not be taken if encryption technology was used to protect the data.

Example

An organisation issues laptops to employees for remote working. An employee saves some documents they need for work onto the laptop. Some of those documents contain personal information such as people's names. The laptop is left on a train or it is stolen. Under the new laws this is a data breach and if the laptop was not encrypted then regulatory action and fines may occur. If the laptop was encrypted then your business is safe from action.

For more information on Encryption visit http://metaphor-it.com/cyber-security/data-security-integrity/