IT POLICY

DEVICE ENCRYPTION

Device Encryption

Desktop and Laptop Encryption

All computers and laptops must be encrypted using approved OCU encryption technologies, this is a mandatory requirement and no exceptions will be granted. Other encryption technologies must not be used as OCU must always be in a position to decrypt and secure Company machines. OCU must hold all encryption keys.

Secure Transfer of Files

If you are transferring data relating to the company, people or clients that is confidential, this should be done by using OCU approved Third party services SharePoint or OneDrive this means that your files will be encrypted and appropriately secured.

File Server Encryption

Encryption of data on file servers, SANs and other central systems is not currently part of the scope of the OCU encryption project. However, if there is a legal or regulatory requirement, or the data is deemed high risk (medical records or client product data for example); a file server encryption solution may be sourced via OCU IT. Companies should contact the Head of Group IT if they need further guidance or information on file server encryption.

Portable Storage Encryption

Portable media drives including USB sticks must have encryption enabled and have access controlled via a username and password.

Signed.....Date: 15/01/21
Brian Lynch – Head of IT

Signed.....Date: 15/01/21
Vince Bowler - Managing Director