

Data Destruction Policy & Guidelines

NetFM commits to ensuring and overseeing the complete destruction of any decommissioned devices used to hold client data, ensuring that no company or client data is subsequently allowed to be viewed, accessed or used by unauthorised persons or to escape into the public domain.

Any such devices residing in third-party premises will be subject to this same data destruction policy and destruction will be carried out by a designated NetFM employee with no third-party interaction beforehand or subsequently, thus negating the possibility of confidential data/information being shared with, or accessed by, inappropriate or unauthorised third parties.

All employees have a responsibility (under NetFM's Security Policy that they have signed) to ensure that any company equipment they use is stored, accessed, disposed of or destroyed with reasonable care and under sufficient security conditions to avoid unauthorised access.

The Technical Director is responsible for checking, ensuring and documenting that any such device has been terminated, destroyed or disposed of correctly.

Similarly, all employees have a responsibility (under NetFM's Security Policy that they have signed) to ensure that any company or third-party client data that they access, use or view is accessed securely, with all reasonable duty of care taken to avoid unauthorised access.