IT Secure Disposal Policy

This policy applies to all companies within the Relyon Group.

Relyon Services Group ("RSG") holds and processes information and is required to protect that information in line with relevant legislation and in conformity with all applicable regulations and policies such as the Information Security Policy, the Data Protection Policy, and the Records Management Policy. This policy sets out the requirements for staff on the secure disposal of RSG's IT equipment and information.

The disposal of such equipment is due to its need for replacement, upgrade, or because it has become obsolete, surplus or redundant. The following are important factors in equipment disposal:

- IT equipment may contain data or information that must be protected.
- The equipment could represent an existing asset value.
- The equipment may be reused or recycled.
- The equipment must be disposed of safely according to legislation and in an environmentally sustainable way.

RSG aims to ensure that all of its IT equipment is managed effectively, including its disposal. Responsible IT asset management and disposal is essential for compliance with the Data Protection Act 2018.

Objectives

This policy aims to ensure:

- Compliance with Data Protection Act 2018 through secure disposal of personal data.
- Compliance with the Information Security Policy and Records Management Policy.
- Erasure of confidential or sensitive non-personal data to avoid breach of confidence, breach of contract or commercial damage.
- Erasure of software which is under licence to avoid breach of licencing conditions.
- Compliance with WEEE Directive (Waste Electrical and Electronic Equipment) through appropriate disposal of IT equipment.

Responsibilities

It is the responsibility of all RSG staff to ensure that the information held by RSG is disposed of appropriately and that all sensitive information is disposed of securely.

All RSG staff are responsible for compliance with this policy. All staff have responsibilities under the Data Protection Act 2018 and must make all reasonable efforts to prevent any personal data held from being accidently or deliberately compromised.

Our IT subcontractor and the Head of Group Services are responsible for the appropriate destruction or disposal of equipment in compliance with waste regulations and for providing RSG's Finance Department with a record of all such disposal within an agreed timeframe.

Responsibility for and implementation of this policy resides with RSG's Senior Management Team.

Definitions

Secure Disposal

Secure disposal refers to the process by which all information, including information held on IT equipment, is irretrievably destroyed in a manner which maintains the security of the equipment and information during the process and up to the point of irretrievable destruction.

IT Equipment

IT equipment means all computing or related equipment purchased by or provided by RSG to store or process information including but not necessarily limited to: desktop computers, servers, printers, copiers, laptops, tablet computers, electronic notebooks, mobile telephones, digital recorders, cameras, USB sticks, DVDs, CDs and other portable devices and removable media.

Information

Information means all information and data held or recorded electronically on IT equipment or manually held or recorded on paper. For the purpose of this policy, the information held by RSG can be divided into two categories: nonsensitive; and sensitive information. Sensitive information comprises: All personal information and all confidential information, the loss of which would, or would be likely to, cause damage or distress to individuals or to RSG. The default category is that all information is deemed to be sensitive unless specifically identified as otherwise.

Policy

This policy on disposal, covers all data or information held by RSG whether held digitally or electronically, on IT equipment or as manual records held on paper or in hard copy. It is RSG's policy to ensure that all information held by RSG is disposed of appropriately, in conformity with RSG's legal obligations and in accordance with RSG's regulations and Records Management Policy.

It is RSG's policy to ensure that all sensitive information which requires disposal is disposed of securely.

Where information is held on IT equipment, it is the policy of RSG that such information will be assumed to hold sensitive information and that all information residing on such equipment must be disposed of securely.

WEEE: IT equipment must also be disposed of in line with the EU Waste Electrical and Electronic Equipment (WEEE) Directive and the UK Waste Electrical and Electronic Equipment Regulations 2006.

Copyright software must be disposed of in line with copyright legislation and software licencing provisions.

IT Equipment

The main types of IT equipment that can record or hold data, includes:

- PCs
- Laptops
- Mobile phones
- USB memory sticks and external hard drives
- Servers

• Tablets

• Multi-functional devices – printers/scanners

All staff and managers must follow the approved disposal/destruction process for IT equipment to ensure that the risk of any loss of sensitive information or data breach is negated.

Staff holding RSG data on IT equipment should routinely dispose of the data when it is no longer required to be held for legal or contractual purposes or is no longer necessary for the business purpose for which it was originally created or held.

Data deemed to be removed from IT devices or media, involves putting the information in an irretrievable position. Data held in a recycling 'bin' on the device or data which can be easily recovered by the user are not regarded as being 'irretrievable' or 'beyond use' and may still be subject to discovery and disclosure under information law (Freedom of Information, Data Subject Request) or litigation.

Staff should never dispose of RSG IT equipment (device or media) without taking appropriate steps to ensure the irretrievable deletion of data held on the equipment.

Staff should be mindful that RSG mobile phones contain data which will need to be extracted or deleted from the device before the device is disposed of.

Staff responsible for the contracts relating to RSG leasing equipment (such as multi-function copiers) should ensure that the leasing contract certifies the secure disposal of any RSG data held on devices during the period of lease.

Online Data

Online data such as in accounts provided to staff by RSG for the purpose of their employment are not automatically deleted when staff leave the RSG. These accounts are de-activated and access to the data retained for any necessary business purpose. Staff should ensure appropriate management and handover of RSG data prior to leaving RSG.

Physical Information

Hard copy Information and data held in paper or hard copy which contain sensitive information shall be irretrievably destroyed in a way in which the information cannot be reconstituted, by shredding, pulping or incineration.

The process leading to and the process of shredding, pulping or incinerating such information shall be carried out securely.

Where the shredding or incineration are carried out on behalf of RSG by a third party, there shall be a contract with that third party which appropriately evidences:

a) that party's obligations to keep that data confidential and;

b) that party's responsibility under the Data Protection Act 1998 for the secure disposal of the data.

Where hard copy information is stored externally by a third-party data storage contractor, the contract shall ensure secure disposal of the data at a time which conforms with RSG's Retention.