Policy on the Secure Disposal of IT equipment

1. **Introduction**

The Company holds and processes a large amount of information and is required to protect that information in line with relevant legislation and in conformity with legal requirements and policies such as the Information Security Policy and the Data Protection Policy. This policy sets out the requirements for staff on the secure disposal of the Company's IT equipment and information.

2. **Definitions**
2.1 Secure Disposal

Secure disposal means the process and outcome by which 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.

2.2 IT Equipment

IT equipment means all equipment purchased by or provided by the Company 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.

2.3 Information

2.3.1 Information means all information and data held or recorded electronically on IT equipment or manually held or recorded on paper.

2.3.2 For the purpose of this policy, the information held by the Company can be divided into two categories: non-sensitive; 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 the Company.

2.3.3 The default category is that all information is deemed to be sensitive unless specifically identified as otherwise.

3. **Responsibilities**

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

3.2 Responsibility for this policy resides with the Company's Directors. Implementation of this policy is managed through the Companies management meetings who reports to the MD.

4. **Statement of Policy**

4.1 This policy on disposal covers all data or information held by the company whether held digitally or electronically on IT equipment or as manual records held on paper or in hard copy.

4.2 It is the Company's policy to ensure that all information held by the Company is disposed of appropriately, in conformity with the Company's legal obligations.

4.3 In particular it is the Company's policy to ensure that all sensitive information, which requires disposal, is disposed of securely.

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

4.5 The Company supports policies, which promote sustainability and take account of environmental impact. The Company will therefore support recycling or sustainable redeployment in the disposal of IT equipment as long as information held on the equipment is irretrievably and securely destroyed prior to the disposal of the equipment.

4.6 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.

4.7 Copyright: software must be disposed of in line with copyright legislation and software licensing provisions.

5. **Policy Principles**

5.1 Hard copy

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

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

5.1.3 Where the shredding or incineration are carried out on behalf of the Company 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.

5.1.4 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 the Company's Retention Schedule.

5.2 IT Equipment

5.2.1 Since the policy default is that all IT equipment which stores or processes data will be deemed to hold sensitive data, then all such IT equipment will undergo appropriate physical destruction or an appropriate data overwrite procedure which irretrievably destroys any data or information held on that equipment.

5.2.2 Where an overwrite procedure fails to destroy the information irretrievably, the equipment shall be physically destroyed to the extent that the information contained in it is also irretrievably destroyed.

5.2.3 For the avoidance of doubt, removable digital media including but not limited to CDs, DVDs, USB drives, where the default is that they contain sensitive data, shall, if not successfully overwritten, be physically destroyed to the extent that all data contained in the media are irretrievable.

5.2.4 All IT equipment awaiting disposal must be stored and handled securely.

5.2.5 Where the overwriting procedure and/or physical destruction of IT equipment are carried out on behalf of the Company by a third party, there shall be a contract with that third party which appropriately evidences: that party's obligations to keep that data confidential and; that party's responsibility under the Data Protection Act 1998 for the secure disposal of the data.

5.2.6 In any case where IT equipment is to be passed on by the Company for re-use, those staff involved in the sale or transfer of the equipment shall ensure that any information on the equipment has been irretrievably destroyed and that any other appropriate issues, including, but not limited to, the safety of the equipment are satisfactorily addressed.

5.2.7 Photocopiers and printers used or owned by the Company may have a data storage capacity. Where such IT equipment contains information or data, the disposal of such equipment must have due regard to this policy.

6 **Record of Destruction**

6.1 Any third party contracted to dispose of sensitive hard copy information shall certify the irretrievable destruction of the information.

6.2 company staff who have responsibility for the information which is disposed of shall ensure that the disposal conforms with the Company's Retention Schedule and that, where necessary, a record is kept documenting the disposal.

6.3 Where the disposal involves the disposal of IT equipment, the Company shall keep a record of the asset number of the equipment, which has been disposed of along with a record of the process by which the information stored on the equipment has been irretrievably destroyed.

7 **Reporting**

7.1 All staff and other users of information should report immediately to the MD any observed or suspected incidents where sensitive information has or may have been insecurely disposed of.

8 Guidelines

8.1 Hard Copy

8.1.1 Staff holding Company data in hard copy 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. In determining whether and when the data should be disposed of, staff should consult the Company's Retention Schedule

8.1.2 It is good practice to shred, pulp or incinerate all Company data which requires destruction. Where hard copy waste is sensitive data (as defined in 2.3.2) it should always be securely and irretrievably destroyed by shredding, pulping or incineration. In order to ensure the secure and irretrievable destruction of hard copy, staff are required to use the service provided by the Company's selected contractor for the destruction of confidential waste.

8.2 IT Equipment

8.2.1 Staff holding Company 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. In determining whether and when the data should be disposed of, staff should consult the Company's Retention Schedule

8.2.2 Where a decision has been made that data held on IT devices or media should not be retained, the files containing the data should be deleted from those devices. Deletion involves putting the information "beyond use" by the user of the device or media. Data held in a recycling "bin" on the device or data which can easily be recovered by the user are not regarded as being "beyond use" and may still be subject to discovery and disclosure under information law (Freedom of Information, Subject Access Request) or litigation.

8.2.3 Staff shall never dispose of Company IT equipment (devices or media) without taking steps to ensure the irretrievable deletion of data held on the equipment.

8.2.4 Electronic or digital data which have been put "beyond use" by users may still be reconstituted by IT specialists or by forensic computer analysts. This means that when IT equipment (devices or media) are disposed of, the data should be irretrievably destroyed by being overwritten in accordance with the appropriate industry standard,

or - the hard disc containing the data within the equipment or the media containing the data (e.g. CD, USB stick) should be physically destroyed.

8.2.6 Staff should also be mindful that Company or personal mobile telephones contain data, which will need to be extracted or deleted from the device before the device is disposed of.

8.2.7 Where the Company is leasing equipment (such as multi-functional copiers), staff responsible for the contracts should ensure that the leasing contract certifies the secure disposal of any Company data held on the devices during the period of lease.

Approved by Dr Adnan Niazi

Date 5/7/18
Last Reviewed On 03/07/26

Version 1