Policy on the Secure Disposal of IT equipment, assets, endpoint devices and Company held Data

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.

Statement of Policy

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

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. In particular, it is the Company's policy to ensure that all sensitive information, which requires disposal, is disposed of securely. Disposal of the equipment should be completed by the IT & System Administrators with the approval of the CEO/CFO.

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.

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.

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 licensing provisions.

Definitions

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.
The company will verify to ensure whether or not storage media is contained prior to disposal or re-use. Any asset or media containing confidential or copyright information should be physically destroyed or deleted or overwritten using techniques to make the original information non-retrievable.

Information Security Equipment, assets and endpoint devices

These mean, 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.

Information and Data

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 the Company can be divided into three categories: Level 1 – General (non-sensitive); and Level 2 / 3 – Restricted and Secret (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.

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

Responsibilities

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.

Responsibility for this policy resides with the Company's Directors. Implementation of this policy is managed through the Company's management and through their meetings, who report to the CEO.

Policy Principles

In line with NIST SP 800-88 first published in 2006 that provides clear methods of how to delete data in a secure and permanent way, the company feels confident that we have taken all necessary steps to minimise the changes of our data being recovered by third party.

The company follows the removal of data in one of the below three ways:

Clear

Clearing is a sanitization method that involves using software or hardware products to overwrite all user-addressable storage space. Clearing aims to replace written data and potentially sensitive information with random data. Clearing can be applied by using the standard Read and Write commands on your device, and can involve rewriting data with a new value or resetting the device to its factory settings.

Purge

Purging provides more comprehensive sanitization than clearing, as purging protects information against laboratory attacks that use advanced methods and tools to recover data. Some methods of purging include overwriting, block erasing, and cryptographic erasure.

Destroy

Destroying, like purging, protects data from being recovered and after destroying media the device is no longer able to store data. There are many physical techniques for destroying media, such as disintegrating, incinerating, melting, and shredding.

Hard copy

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.

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 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 2018 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 the Company's Retention Schedule.

IT Equipment

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.

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.

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.

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

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 2018 for the secure disposal of the data.

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.

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.

Record of Destruction

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

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.

Reporting

All staff and other users of information should report immediately to the IT System Administrators, who will notify the Company's Info Sec Officers, any observed or suspected incidents where sensitive information has or may have been insecurely disposed of.

Guidelines

Hard Copy

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.

It is good practice to shred, pulp or incinerate all Company data which requires destruction. Where hard copy waste is sensitive data, 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.

IT Equipment

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

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.

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.

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.

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.

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.

Destruction of Data

Interr shall safely destroy or delete all Personally Identifiable Data contained in the Client or Employee Data and it is no longer needed for the purpose for which it was obtained. Certain types of data may also be exempt from the standard terms. For example, because it's needed for evidentiary reasons in a legal dispute around the contractual breach, because it has been requested by law enforcement, or just complexities due to the particular nature of the service.

Policy Review and Assessment

This policy may be amended by Interr at any time to take into account changes in legislation and best practice. This policy was last reviewed and agreed by the Board and seeks to be reviewed and updated annually. Any queries arising regarding this policy should be addressed to Mick Tabori.

Mick Tabori - CEO
January 2024