Holst
WORKPLACE EFFECTIVENESS

HOLST - DATA DESTRUCTION POLICY

1. OVERVIEW

Personal data in manual (paper-based) format, and the technology equipment on which such data is stored in electronic (automated) format, cannot simply be thrown away. Proper disposal of equipment is both environmentally responsible and required by law.

Paper files, hard drives, USB drives, CD-ROMs and other storage media contain various kinds of Holst data, some of which is considered both commercially and personally sensitive. In order to protect the data, all storage mediums must be properly disposed of. Electronic media should also be 'wiped' prior to being appropriately destroyed, to remove any risk that confidential or sensitive data remains retrievable.

However, simply deleting or even formatting data is not considered sufficient. When deleting files or formatting a device, data is marked for deletion, but is still accessible until being overwritten by a new file. Therefore, special tools must be used to securely erase data prior to equipment disposal.

Holst is aware of its obligations under the GDPR to retain personal data in a safe and secure manner for as long as necessary, and to then dispose of such data in an appropriate manner.

This Data Destruction Policy outlines Holst's approach to fulfilling such obligations.

2. PURPOSE

This policy has been developed to define the requirements for proper disposal of manual and electronic data at Holst.

3. SCOPE

This policy applies to all personal data held by Holst in both manual and electronic formats.

4. POLICY

4.1 Manual Data Disposal

1. Holst will schedule a regular review of its retention of manual records, and will schedule timely destruction of paper-based records where retention has exceeded Holst's operational requirements and Regulatory obligations.
2. These manual records will be collected and stored in a secure environment, prior to destruction;
3. Holst will make paper cross-cut shredders available within the organisation in order to dispose of paper records which have no, or short-term retention periods – this may

include (but are not limited to) general office correspondence, hand-written notes used prior to transcription, copies of documents which might have been used for short-term cross-reference, etc.

4. Staff will be trained and aware of their obligation to shred such material using these in-house shredders.
5. For the bulk disposal of paper records for which there is a medium- to long-term retention obligation, Holst will appoint an appropriately specialised third party to process the act of destruction of these records, using approved and recognised industry standard methods;
6. The third party will be required to sign an appropriate Data Processor contract, as per requirements from [the appropriate legislation];
7. This third party will be required to security vet all staff involved in the process of data destruction, to BS:7858 Security screening of individuals employed in a security environment. Code of Practice standard, including (where appropriate) police-based security clearance;
8. In order to minimise the risk of inadvertent loss or disclosure, all manual records due for destruction should be shredded as soon as possible once their retention has exceeded the respective retention obligation;
9. The following steps will be required for the effective destruction of manual data:
    a) Collation of the paper records to a designated and secure Holst site;
    b) Ensure the third party takes full responsibility for the collection and (where necessary) removal of the records from the designated Holst site;
    c) Ensure the third party tags all equipment prior to destruction;
    d) Ensure the third party provides a sufficient number of personnel to ensure that the records can be removed and shredded as quickly, efficiently and securely as possible;
    e) Ensure the third party records some level of inventory of the paper records on site, prior to commencement of the destruction process;
    f) All records to be placed in secure bags or cartons, prior to loading on to a vehicle for on-site destruction, or transport to a remote site for same;
    g) The appointment of appropriate Holst staff to witness the shredding/decanting of all records and the security of the vehicle and/or remote site, for the purpose intended;
    h) Ensure the shredding of all redundant paper records are reduced to cross-cut debris no larger than [appropriate dimensions] in surface area;
    i) The third party will issue an appropriate and valid Certificate of Destruction;
    j) The third party will be required to provide a clear documented action plan, with escalations, in the event of any major or minor incident that may impact the fulfilment of the shredding service;
    k) The third party will account for the environmentally-friendly disposal of the shredded materials, to the satisfaction of Holst, as a final phase of this destruction process.

4.2 **Technology Equipment Disposal**

1. Holst will schedule a regular collection of end of life technology equipment, throughout the organisation. This equipment will be collected and stored in a secure environment, prior to destruction;
2. Technology equipment included in the scope of this policy are:
    a. Internal Hard Drives (Physical/SSD);
    b. External hard Drives (Physical/SSD);
    c. RAM Modules;
    d. Tapes (DAT/DLT/LTO);
    e. CD/DVD/Blu-ray;
    f. Mobile Phones/PDAs;
    g. USB Sticks;
3. Holst will appoint an appropriate third party to process the act of destruction of this equipment, using approved and recognised industry standard methods;
4. The third party will be required to sign an appropriate Data Processor contract, as per requirements from the [appropriate legislation];
5. The third party will be required to security vet all staff involved in the process of data destruction, to BS:7858 Security screening of individuals employed in a security environment.
6. Code of Practice standard, including police based security clearance;
7. All destruction must be same day;
8. The following steps will be required for the effective destruction of technology equipment:
    a. Collection of the equipment from a designated and secure Holst site;
    b. Ensure the third party takes full responsibility for the packing and removal of equipment from the designated Holst site;
    c. Ensure the third party tags all equipment prior to destruction;
    d. Ensure the third party provides a sufficient number of personnel to pack and remove the equipment, so that the equipment can be removed as quickly, efficiently and safely as possible;
    e. Ensure the third party delivers, fills and removes full storage boxes and cages on the same day;
    f. Ensure the third party completes an asset registry count on site, prior to commencement;
    g. All equipment to be placed in security boxes and sealed, prior to loading on to a vehicle for on-site destruction, or transport to a remote site for same;
    h. The appointment of appropriate Holst staff to witness the shredding/decanting of all equipment and the security of the vehicle and/or remote site, for the purpose intended;
    i. Ensure the destruction of all redundant media to debris no larger than 20mm in diameter;

j. The third party will issue an appropriate and valid Certificate of Destruction;
k. The third party will be required to provide a clear documented action plan, with escalations, in the event of any major or minor incident that may impact the fulfilment of the service;
l. The third party will account for the environmentally-friendly disposal of the shredded materials, to the satisfaction of Holst, as a final phase of this destruction process.

5. HOLST RAMIFICATIONS

Holst is very much aware of its responsibilities towards the personal data within its care, whether in manual or electronic format. Holst is equally aware that failure to properly dispose of such data can have several negative ramifications to Holst, including regulatory investigations, fines and penalties, negative customer perception, reputational damage and costs associated with notifying concerned parties of data loss and/or inadvertent disclosure.

6. DEFINITIONS

BS:7858	Standard for security screening of employees
Certificate of Destruction	A legal document showing that all materials that have been handed over to the custody of a destruction service provider have been destroyed.
Data Inventory	A comprehensive list of the material (whether paper-based or electronic) which is subject to destruction.
Data Processor	A third party contracted to process data on behalf of another party.

7. REVISION HISTORY

Version	Reason for Change
1.0	Document creation
2.0	Re-branded with new logo