Company Data Security Policy for:

Holcombe Occupational Hygiene Services Ltd.

Signed:

Martin Dippnall - Managing Director

Holcombe Occupational Hygiene Services Ltd.

Date: 26th July 2023

Review date: August 2024

Document number: HSM/002/1.4/07/23

1. Policy statement

1.1. Holcombe Occupational Hygiene Services Ltd. recognises the importance of adequate data security to protect the privacy and commercial interests of its customers.

1.2. Therefore steps are taken to:

a) Classify all data
b) Implement appropriate data security measures dependent on the data classification level
c) Ensure data is retained for the minimum amount of time
d) Data is securely destroyed when appropriate

2. Data categories

Information classification	Description	Examples	Data handling
Highly Confidential	Highly sensitive data containing personal information	• Medical records • Personal addresses, phone numbers, NI numbers • Birth & Death certificates • Damage schedules • Individual claim data • Individual biological monitoring data • Payroll data • Pension data	Full data security procedures (below)
Confidential	Sensitive data containing confidential information	• Anonymised or group claims data • Occupational hygiene reports • Personal exposure monitoring records • Customer financial data	
Internal Use Only	Data not meant for general release	• HOHS Ltd. invoices • Company / customer contact details (phone numbers, email and contact names etc.)	Data will not be shared with third parties, unless subject to a statutory request.
Unclassified	Reports and data freely available from libraries and/or the internet	• Research papers, company reports	None

3. Data types held

3.1. Occupational Hygiene project files will typically consist of a survey report, monitoring data files, paper handwritten site notes, site plans, survey photographs, chemical data sheets, analysis results etc.

3.2. Civil litigation claims will contain a case file provided by the Instructing Solicitor. The case file contains private information pertaining to the Claimant/Pursuer and/or Plaintiff, and/or their spouse and/or close family members; as well as disclosed documents by the Defendant/ Defender in the case. We therefore process sensitive classes of information that may include, for example:

a. Birthdate and home address of Claimant/Pursuer and/or Plaintiff and/or their spouse. Names and home addresses of other family members
b. Family, lifestyle and social circumstances of Claimant/Pursuer and/or Plaintiff and/or their spouse
c. Educational details of Claimant/Pursuer and/or Plaintiff
d. National Insurance number and NI history of Claimant/Pursuer and/or Plaintiff
e. Employment history of Claimant/Pursuer and/or Plaintiff
f. Employment contracts, personnel files and/or employment disciplinary records
g. Employee training records
h. Personal witness statements
i. Medical histories, hospital records, medical imagery and GP notes of Claimant/Pursuer and/or Plaintiff and/or spouses
j. Private financial details including wage data/payslips, pension data, and private bank account details
k. Occupational health notes, records and logs of Claimant/Pursuer and/or Plaintiff
l. Corporate health and safety policies

4. Full data security procedures

4.1. The Managing Director has overall responsibility for the Company Data Security Policy within the organisation.
4.2. Home office comprises of a separate room with lockable door, lockable filing cabinet and is fully covered by a building security alarm.
4.3. All data will only be used for the intended purpose.
4.4. All customers' electronic data to be held within a single customer-specific folder on an encrypted laptop, with subfolders for project-specific information. A single back-up will be made on an encrypted USB stick (AES 256-bit encryption) which is kept locked in a cabinet. Backup will be run from time-to-time e.g. monthly. The back-up will not be removed from the fixed site.
4.5. All customers' paper data to be stored within a separate labelled folder in a locked area, when not in actual use.
4.6. All customers' data to be stored for the minimum time necessary and thereafter will be permanently destroyed using either a paper-shredder or an electronic 'shredder' program.
4.7. Electronic report delivery will be by a password-protected file.
4.8. When ready to be archived (3 months after report delivery) project files will consist of the final published report only, together with invoicing details. The report file will be kept indefinitely, together with a single back-up as described above. **All other data files held by HOHS ltd will be permanently destroyed,** unless longer-term storage is specifically requested by the customer.
4.9. Data will not be shared with third parties, unless subject to a statutory request.

5. **Data loss**

5.1. In the unlikely event of a data loss, the effected customer will be informed as soon as possible, within a reasonable time frame.

6. **Registration**

6.1. HOHS ltd is registered in the Information Commissioner's public register of data controllers.

7. Review

7.1. This policy is subject to an annual review.

~End of document~