Data Protection Policy
(HP008)

1. PURPOSE

The purpose of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures in their day to day practice.

2. PRINCIPLES

- Hoople will comply with the requirements of Data Protection legislation.
- Hoople will promote privacy and data protection compliance at all times and implement measures that meet the principles of data protection by design and data protection by default, including data minimisation, transparency, and creating and improving security features on an ongoing basis.
- Hoople will maintain evidence of compliance with Data Protection laws.
- In line with the Data protection regulations, all personal data will be:
    - Processed lawfully, fairly and in a transparent manner.
    - Collected for specified, explicit and legitimate purposed and no further
    - Adequate, relevant and not excessive
    - Accurate and where relevant kept up to date
    - Not kept for longer than necessary
    - Processed in accordance with the data subject's rights
    - Kept secure at all times against unauthorised or unlawful loss or disclosure
    - Not transferred to other countries without adequate protection
    - Only transfer personal data to other organisations where appropriate agreements are in place
- All personal information will be processed in line with Data Protection regulations.
- All personal and special categories of personal data will comply with a lawful category as specified within the Data Protection regulations.
- Criminal offence data will be dealt with in a similar way to special category data and will be processed in accordance with legislation.
- All personal information will not be used apart from for the exact purpose for which permission was given and not disclosed to others unlawfully.
- All members of staff will complete the Hoople Mandatory data protection training.
- Employees have a responsibility to adhere to data protection regulations at all times.
- All members of staff are responsible for reporting any breach or potential breach to their line manager / EMT member as soon as they become aware of the breach or potential breach.
- Should a breach in Data Protection occur this will be investigated and acted upon promptly.
- Hoople will maintain a log of all reported data protection breaches, where required the ICO will be notified of a data protection breach within 72 hours where this feasible.
- If the unlikely event that a breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, Hoople will promptly inform those individuals affected. All queries about handling personal information will be dealt with swiftly and politely.
- Individuals rights to request will be dealt with in a swiftly and politely.

- Hoople will take appropriate technical and organisational steps to ensure the security of personal data.
- Data protection impact assessments will be carried out where appropriate as part of service / systems design/ redesign and planning of projects, systems and programmes.
- Hoople will implement appropriate technical and organisational measures that include internal audits of processing activities, maintaining relevant documentation on processing activities.
- Hoople will maintain the required data protection documentation as required by data protection legislation, this includes and is not limited to privacy notices, Data audit logs, data processing agreements, data sharing agreements, document retention schedules,
- Data protection documentation will be reviewed and updated upon any major change in service, or at least every three years whichever is the sooner.

3. DEFINITIONS

3.1.1 **Personal Data** (sometimes referred to as Person Identifiable Information - PII).

Any information relating to a person (a 'data subject') who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person i.e.

- Name
- Address
- Date of birth
- NHS Number
- National insurance number
- Carers details
- Next of kin details
- IP Address (used to identify devices on a computer network)
- email address

3.1.2 **Sensitive/ Special Data**

- Racial /ethnic origin
- Political opinion,
- Philosophical or religious beliefs,
- Trade union membership,
- Genetic and biometric data,
- Health data,
- Sex life and sexual orientation data.
- Criminal data.

3.2 **Data Subject** - The identified or identifiable living individual to whom personal or special category data relates.

3.3 **Data Controller** - The natural or legal person, public body, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

3.4 **Data Processor** - A person, public body, agency or other body which processes personal data on behalf of the controller.

3.5 **Processing** - In relation to personal data, means any operation or set of operations which is performed on personal data or on sets of personal data (whether or not by automated means, such as collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, use, disclosure, dissemination, restriction, erasure or destruction).

3.6 **Recipient** - This refers to any person or organisation to which data is disclosed.

The Personal Data Guardianship Code suggests five key principles of good data governance on which best practice is based. Hoople seeks to abide by this code in relation to all the personal data it processes, i.e.

- **Accountability:** those handling personal data follow publicised data principles to help gain public trust and safeguard personal data.
- **Visibility:** Data subjects should have access to the information about themselves that an organisation holds. This includes the right to have incorrect personal data corrected and to know who has had access to this data.
- **Consent:** The collection and use of personal data must be fair and lawful and in accordance with data protection principles. Personal data should only be used for the purposes agreed by the data subject. If personal data is to be shared with a third party or used for another purpose, the data subject's consent should be explicitly obtained.
- **Access:** Everyone should have the right to know the roles and groups of people within an organisation who have access to their personal data and who has used this data.
- **Stewardship:** Those collecting personal data have a duty of care to protect this data throughout the data life span.

4. SCOPE

The policy and related procedures apply to all employees of the organisation and also applies to secondees, contractors, agency workers engaged by Hoople.

Methods for processing information include all medium including but not limited to electronic and paper records

5. ROLES AND RESPONSIBILITIES

5.1. Data Protection Officer

The Data Protection Officer is responsible for the following tasks:

- Informing and advising Hoople EMT, any processor engaged by Hoople as data controller, and any employee of Hoople who carries out processing of personal data, of that person's obligations under the legislation,
- Produce and deliver training packages to ensure staff are fully aware of their responsibilities under current legislation
- Audit processes and procedures to ensure that staff both understand and comply with their responsibilities under current legislation.
- Providing advice and monitoring for the carrying out of a data protection impact assessments,
- Co-operating with the Information Commissioner's Office,
- Acting as the contact point for the Information Commissioner's Office,
- Monitoring compliance with policies of Hoople in relation to the protection of personal data,

- Monitoring compliance by Hoople with the legislation.
- Reminding Board members and all Hoople staff of their responsibilities under the Data Protection Act.

In relation to the policies mentioned above, the data protection officer's tasks include—

(a) Assigning responsibilities under those policies,

(b) Raising awareness of those policies,

(c) Training staff involved in processing operations, and

(d) Conducting audits required under those policies.

The Data Protection Officer is also responsible for the oversight of the Information Governance and Information Access functions.

Hoople will provide the Data Protection Officer with the necessary resources and access to personal data and processing operations to enable them to perform the tasks outlined above and to maintain their expert knowledge of data protection law and practice.

5.2 Hoople Board

The Hoople Board are responsible for ensuring that the organisation complies with its responsibilities under the Data Protection Act through monitoring of activities and incidents via reporting by the Data Protection Officer. The Board will also ensure that there are adequate resources to support the work outlined in this policy to ensure compliance with the Data Protection Act.

5.3 Executive Management Team

The Executive Management Team will be responsible for discussing and resolving and data protection and confidentiality issues which may arise, approve information governance and information access policies, monitor activities and incidents via monthly reporting by the Data Protection Officer and escalate issues where appropriate to Hoople Board.

5.4 Hoople employees.

All Hoople employees will ensure that:-

- Personal information is treated in a confidential manner in accordance with this and any associated policies.
- The rights of data subjects are respected at all times.
- Privacy notices will be made available to inform individuals how their data is being processed.
- Personal information is only used for the stated purpose, unless explicit consent has been given by the Data Subject to use their information for a different purpose.
- Personal information is only disclosed on a strict need to know basis, to recipients who are entitled to that information.
- Personal information held within applications, systems, personal or shared drives is only accessed in order to carry out work responsibilities.
- Personal information is recorded accurately and is kept up to date.
- They refer any subject access requests and/or requests in relation to the rights of individuals to the Data Protection Officer.
- They raise actual or potential breaches of the Data Protection Act to the Data Protection Officer as soon as the breach is discovered.
- Promote privacy and data protection compliance at all times.

- Data Protection Impact Assessments are carried out as appropriate.

It is the responsibility of all representatives and staff to ensure that they comply with the requirements of this policy and any associated policies or procedures.

6. COMPLIANCE

Failure to follow the policy may impact on good employee relations and the reputation of Hoople Ltd. Appropriate action (including disciplinary) will be taken if the policy is breached.

Managers who are contractors, agency workers or individuals otherwise contracted to work for Hoople Ltd and who fail to consistently apply this policy may have their contracts terminated without notice.

7. SUBJECT MATTER EXPERT SUPPORT / ADVICE

Subject matter expert advice in relation to any Data Protection query is available to Hoople the Data Protection Officer: data.protection@hoopleltd.co.uk

8. REVIEW

This policy will be reviewed after 3 years or earlier if required.

Document control

Policy approved by	EMT	*Date approved*	20/05/2024
Implementation date	20/05/2024	*Review date*	May 2027

Change Log

Issued	Date	Description of Change	Reason For Change	Pages affected
v0.1	Jan 15	Draft for approval		
V1.0	April	Feedback from Hoople Policy group	Feedback from Hoople Policy group	All
V2	Feb 17	None	Scheduled review	None
V3	Sept 17	Inclusion of accessibility of Subject Matter expert advice	Recommendation from ISO27001 audit	Page 2
V4	April 18	Full review	Introduction of GDPR legislation	All
V5	May 21	General update	Scheduled review	All
V6	November 21	General update and logo	Scheduled review	Page 1, 2 & 3
V7	March 2024	Full review and update	IG Manager Feedback	All