Data protection and security Policy

1. Overview

1.1 All employees, consultants, officers, contractors, interns, volunteers, agency and casual workers are covered by this policy which commits Aesop to meeting Data Protection legislation and to protect the privacy of information held in the process of operating its services.

1.2 Data Protection is a legal requirement of all organisations collecting and using personal information and there are significant legal, financial and reputational consequences of failing to operate to the highest information and data protection standards.

1.3 This policy should be augmented with further guidance and policies on Record Keeping and IT & Cyber Security, as the operating model matures.

1.4 This policy applies in all locations and operating premises. Importantly the policy must be maintained when at home or travelling as this may represent a significant risk to data protection.

1.5 In short, Aesop commit to uphold fair and lawful data management and protection in line with prevailing legislation (currently GDPR[1]).

1.6 The trustees/board will seek assurance of compliance with this policy through half yearly positive reporting and in-between times by notification of exceptions and breaches.

[1] General Data Protection regulation EU 2016/679 and UK Data Protection Act 2018.

2. What is Data Protection?

2.1 Data protection is defined relative to personal and sensitive data within the seven principles behind GDPR.

- Data will be collected and processed lawfully, fairly and transparently.
- Purpose limitation – collected and processed for specific legitimate reasons.
- Data minimisation –the minimum data collected for the purpose stated.
- Accuracy – care is taken to collect and maintain accurate and up to date records.
- Storage limitation – records are kept only for as long as justifiable by the purpose for collection.
- Integrity and confidentiality (security) – manage personal information in a secure and confidential manner including safe destruction.
- Accountability – Aesop are the data controller and must take accountability for the data it collects and uses as well as ensuring data processors it contracts work within clear processing agreements.

3. What we will do to comply with the principles and law

3.1 Existing data processing will be documented, and a central "record of processing" kept of what is collected, for what reason and for how long it will be retained.

3.2 Any new data processing will be subject to a Data Protection Impact Assessment (DPIA) to ensure we have considered the GDPR principles and made a conscious decision to process the right amount of information for a clear purpose. This will include:

- Clear purpose for collection/processing
- What will be collected
- How and where it will be processed by us or our agents (under a Data Processing Agreement)
- How long the data will be held
- How the confidentiality will be maintained.

3.3 We will be clear (through a Data Processing Agreement) with any partner organisation that we use to process data on our behalf as to the extent of processing permitted and our requirement for them to uphold our confidentiality and processing control.

3.4 We will ensure our paper and electronic record keeping is secure and robust through implementation of an IT and Cyber Security policy.

3.5 We will ensure all staff and those working with us through grant or agency arrangements are aware of the basics of information security and data protection.

3.6 We will be clear with users of our services what we are doing with their data and help them in the event of a query or correction.

3.7 We will maintain registration with the Information Commissioner's Office (ICO) and report breaches and data loss in line with prevailing legislation.

3.8 We will define clear roles and training needs for staff.

4. Roles and responsibilities

4.1 The following are defined roles with respect to Data Protection and not necessarily job titles or whole-time equivalent roles.

4.2 All Staff: required to uphold high standards of security and confidentiality for information they are in possession of or come across in the execution of their duties. At induction and then annually, they will be invited to comply with and support the policies of the organisation. Basic data protection awareness will be given to all staff.

4.3 Data Protection Officer: the primary operational expert for the organisation and will:

- Provide advice on the data protection responsibilities of Aesop and handle any impact arising from changes in legislation.
- Monitor compliance with the regulations, including the assignment of responsibilities, awareness raising, and training of staff involved in the processing operations and the related audits.
- Be the first point of contact for the ICO and for data subjects.
- Lead on responding to Subject Access Requests and Rights to be Forgotten.
- Lead on DPIAs.

4.4 Caldicott Guardian: responsible for championing data protection and confidentiality issues for patients and users of the services Aesop provide.

4.5 Chief Executive: overall accountability for information governance including data protection.

4.6 SIRO (senior information risk owner): required to look across security, risk and data protection issues to ensure prevention and issues management is handled.

4.7 Board: required to provide governance oversite and seek assurances that the policy is being enacted effectively.

5. Data Subjects' rights

5.1 Data Subjects are entitled under data protection law to the following:

- Transparency from Aesop on what is collected, why it is collected and who processes it.
- Access to data held by Aesop about them.
- Correction or erasure of data held about them.

5.2 To help support these rights Aesop will have a privacy statement, issue briefing notes to support data collection from patients/participants, and secure written agreements with any agency processing data on Aesop's behalf.

5.3 Applicants, staff and direct volunteers will have their rights clearly stated in application and induction material.

5.4 There will be a clearly identified contact point within AESOP (signposted on the web site) to whom subject access and data privacy issues can be addressed.

6. How we will assure compliance

6.1 A four-step approach will help us ensure that this policy is complied with.

a. Board of Trustees will reserve annual and 6 monthly agenda slots specifically to review Data Protection: policy; status; training and any breaches or data confidentiality concerns.
b. We will be clear on accountabilities relating to data protection and secure access to specialist advice and guidance in the ongoing review of our policies and procedures.
c. We will make Data Protection awareness mandatory education for all staff and ensure all our partners work to the same education standards.

d. We will ensure that we are transparent about the data we hold regarding service users, donors, staff, and public. Where subjects require access, we will respond openly and correct errors promptly.

September 2021