Model Policy
Information Security and Data Protection

INFORMATION SECURITY AND DATA PROTECTION POLICY

1. Introduction

Carelight Healthcare processes personal data in relation to its own staff and individual client member/ potential member contacts. It is vitally important that we abide by the principles of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 set out below.

Carelight Healthcare holds data on individuals for the following general purposes:

- Staff Administration.
- Advertising, marketing and public relations.
- Accounts and records.

The data will be processed compliant with the principles of fair processing in Article 5, GDPR. Carelight Healthcare will:

- Be transparent in relation to employees.
- Tell employees what we are collecting the data for and be specific about what our purposes for processing data are.
- Only collect what we need for the stated, legitimate purposes.
- Keep the personal data up to date and accurate – inaccurate data will be deleted or rectified.
- Not keep data in a form that allows identification of the data subject for longer than is necessary for the legitimate purposes notified to the employee.
- Keep the data secure.

Personal data means data, which relates to a living individual who can be identified from the data or from the data together with other information, which is in the possession of, or is likely to come into possession of, Carelight Healthcare. Data will only be processed in compliance with the following legal bases:

- Legitimate interest.
- Legal obligation.
- Consent.

Data will be reviewed on a regular basis to ensure that it is accurate, relevant and up to date.

Employees are responsible for ensuring that any changes to old or inaccurate data takes place in a timely fashion. In addition, all employees should ensure that adequate security measures are in place. For example:

- Computer screens should not be left open by individuals who are accessing personal information.
- Passwords should not be disclosed.
- Personnel files and other personal data should be stored in a place in which any unauthorised attempts to access them will be noticed. They should not be removed from their usual place of storage without good reason.
- Personnel files should always be locked away when not in use and when in use should not be left unattended.
- Care should be taken when sending personal data in the mail.
- Destroying or disposing of personal data counts as processing. Therefore care should be taken in the disposal of any personal data to ensure that it is appropriate.

Data subjects, are entitled to obtain access to their data on request. All requests to access data by data subjects i.e. staff or members, should be referred to the Magreth Seka. Where a request is granted, the information will be provided within 30 days of the date of the request.

Any requests for access to a reference given by a third party must be referred to Magreth Seka and should be treated with caution even if the reference was given in relation to the individual making the request. This is because the person writing the reference also has a right to have their personal details handled in accordance with data protection laws, and not disclosed without their consent.