Company Name: George Springall Homecare Partnership

GEORGE SPRINGALL
HOMECARE

Leading the way in outstanding care

Policy No: 03-1506	**Authorised: Roxane Schatara**	**Date:15/05/2018**

INFORMATION SECURITY POLICY

This Policy defines the responsibilities for information security within the Organisation, the steps to be taken to guard against risks, and the action to be taken in the event of a breach of security. This Policy applies to all staff with access to Company data and / or information systems, and to all types of data (paper-based and electronic) and information systems:

A: POLICY OBJECTIVES:

1. To provide assurance to all staff members that the data they use:

   - is available and can always be accessed;
   - has integrity, and has not been deliberately or inadvertently modified from an approved version;
   - is kept confidential; i.e. sensitive information is only available to those persons authorised to have access;
   - can be produced in order to comply with legitimate requests from law enforcement agencies, from data subjects as defined by the *Data Protection Act 1998*, and in any other circumstances for which there is current or future legal provision.

2. To ensure protection against risks, including but not limited to:

   - loss or damage to Company finance, personnel and service user records;
   - damage to reputations caused by breaches of security;
   - liability for the consequences of breaches of security.

3. To provide appropriate staff training in the awareness of the need for security, the measures taken to achieve this, and the consequences of security breaches. Additional specialist training will be provided to staff members who have responsibility for the IT systems.

B: RESPONSIBILITIES:

1. Registered Manager retains overall responsibility for over-seeing the implementation of this Information Security Policy. In particular this will include ensuring that appropriate security measures are in place for centrally-provided IT systems, the IT infrastructure systems, and the Company-wide management information systems.

2. Individual Managers (or other named staff members) are responsible for ensuring that appropriate security is in place to protect data and information systems under their control, and for taking action when appropriate. This will focus upon physical security for access to rooms, filing cabinets and computers. Systems and procedures are in place to protect the security of both paper-based and computer-based information, and the mechanisms for responding and assisting in investigations in the event of a security breach.

3. All staff with access to information must take all precautions to protect data held within the Organisation, to here to the principles of the *Data Protection Act 1998*, to ensure that confidentiality of data is respected, and to comply with any guidelines that may be issued by the Organisation. Additional *Policy Nos 1500, 1501, 1503, 1504, and 1505* also refer.

4. Registered Manager will carry out an annual audit or risk assessment on all information for which the Organisation is responsible, and take action to ensure that security measures are in place that are up-to-date and consistent with the risk assessment. The risk assessment will focus upon the physical security of equipment, systems security, access to data, and Disaster Recovery Plans (ref *Policy No 4300)*.

C: HANDLING BREACHES OF I.T. SECURITY:

1. The risks associated with using IT systems connected to the Internet are considerable. Breaches of security affecting electronic information include the following situations:

   - loss of data;

   - inadvertent release of data to unauthorised persons;

   - unauthorised access to one or more information systems which may affect the security of the system itself.

2. Any person suspecting a breach of IT security should report the matter immediately to the Registered Manager. Where a breach of security is confirmed the Registered Manager will undertake a full investigation. A full report on the actions taken, lessons learned and an action plan for improvements will be issued for staff awareness.

3. Following successful remedy of a breach the Registered Manager will delegate a named staff member to take responsibility to actively monitor the Organisation's IT network and periodically probe for security breaches and weaknesses within permissible limits, and to report their findings to the Registered Manager.