Company Name: Integrative Supported Living Care

Policy No: 03-1519	Authorised: Pellagia Margolis	Date: 15/01/2020

POLICY ON THE *DATA PROTECTION ACT 2018*

This Policy defines the arrangements in place within the Organisation that assures compliance to the requirements of the Data Protection Act 2018*, as relevant to the Organisation's business interests. This Policy should be read in conjunction with Policy No 1514 on the* General Data Protection Regulations (GDPR)*:*

A: INTRODUCTION:

1. The *Data Protection Act 2018* addresses certain requirements for all Organisations that collect and process personal data as part of their on-going business operations. Personal data is defined as any information relating to an "identifiable living individual", and will therefore apply to the Organisation's service users, employees and suppliers.

2. The *Data Protection Act 2018* applies to any data recorded in a filing system that allows personal data to be easily accessed.

3. The *Data Protection Act 2018* applies to records kept in hard copy (paper) format, and as computer / biometric files.

B: PRINCIPLES OF DATA PROTECTION:

B.1 The way in which the Organisation handles and manages service user information will conform to the following 6 information management principles, ref the *GDPR:*

1. Justify the purpose(s) of using confidential information;
2. Only use it when absolutely necessary;
3. Use the minimum that is required;
4. Access should be on a strict need-to-know basis;
5. Everyone should understand his or her responsibilities;
6. Understand and comply with the law.

B.2 The Organisation is committed to the enforcement of the following *GDPR* Code of Good Practice in relation to the data it retains on service users and employees. In summary, data will:

- be fairly and lawfully processed;
- be used for a limited and well-explained purpose;
- be relevant to the Organisation's needs;
- not be unnecessarily excessive in detail;
- be accurately maintained;
- not be kept any longer than is necessary, or required by law;
- only be used in accordance with the individual subject's rights;
- be securely stored;
- only be made available to authorised persons (see section C.4 of this Policy).

B.3 In this respect the following additional policies within the Organisation's documentation system are relevant:

- *Policy No 1500: Control of Records & Service Users' Access to Personal Files*
- *Policy No 1501: Records Maintained at the Service User's Home*
- *Policy No 1505: Confidentiality Policy*
- *Policy No 1506: Information Security Policy*
- *Policy No 1508: Electronic Communications Policy* - Code of Practice
- *Policy No 1514: GDPR Policy*

Policy No: 03-1519	Authorised: Pellagia Margolis	Date: 15/01/2020

POLICY ON THE *DATA PROTECTION ACT 2018*

- *Policy No 1516:* *Data Breach Policy*
- *Policy No 1517:* *Subject Access Request (SARs) Policy*
- *Policy No 1518* *Cybersecurity Policy*
- *Policy No 4300:* *Business Continuity Planning Policy*

C: POLICY DETAILS:

1. The Organisation will require written consent from the subject individual in order for personal data to be collected and processed. In this respect it will be taken that consent is implied through the following:

   1.1 *Service users* - by the service user accepting the Contract for Care, which is signed by the service user or authorised representative. In order for the Organisation to develop an appropriate Plan of Care personal details must be divulged and kept on record. In this respect *Policy Nos 1500 & 1505* (above) are relevant.

   1.2 *Employees* - by completing the Job Application Form at onset of employment, and where the employee has not registered an objection to their data being used.

2. *Registration under the Data Protection Act 2018* - as a fundamental requirement the Organisation will check with the Data Commissioner as to whether the type of personal data held on service users and employees requires a formal registration to be in place.

3. All individuals, service users and employees, have the right of access to manual and computerised records concerning their personal data. For service users, this is supported by *Policy No 1500.*

4. Where it is deemed necessary to divulge personal data to a third party this will only be done with the express permission of the individual subject, ref. *Confidentiality Policy, No 1505. In this respect both staff and service users / relatives / advocates will also be advised that personal information held by the Organisation may be shared with the Registration / Regulating Authority, as appropriate.*

5. Personal data and records will be maintained under appropriate conditions of security to prevent any unauthorised or accidental disclosure. Records can be hard copy (paper) format and electronic (word processed, scanned *pdf,* and biometric format) files. In each case *Policy No 1500* refers, and particular attention is paid to the following aspects of records storage:

   5.1 Hard Copy (paper) files:

   - location of storage;
   - identification of those employees authorised to have access;
   - responsibilities for secure storage;
   - retention times; i.e. how long records are kept for (archived);
   - methods of disposal of out-dated sensitive documents (cross-cut shredding / incineration).

   5.2 Electronic (computer) files:

   - responsibilities for implementing security systems for computer files;
   - encryption / password-protection for access to sensitive data files;
   - who is authorised to have knowledge of these passwords;
   - how often encryption / passwords are changed;
   - implications for networked systems;
   - how long records are kept for;

- back-up, control and management of what are essentially copies of personal data.

6. When personal data is being processed, administrative staff will take all reasonable precautions to prevent access of data by unauthorised persons:

6.1 Record files are locked away when not in use.

6.2 Where practical, VDU screens should be tilted towards the user and away from the general office environment.

6.3 VDUs are not left on when not in use.

6.4 Manage a "clear desk" policy for personal office housekeeping.

6.5 Ensure that confidential conversations are not overheard.

6.6 Ensure information is transported securely.

6.7 Ensure that sensitive data is encrypted / password protected.