CONFIDENTIALITY POLICY

1.0 INTRODUCTION

1.1 We recognise that we have:

- a responsibility to treat all information regarding service users, Directors and employees as confidential, and
- a duty to ensure that personal and other sensitive information is recorded, stored and processed in compliance with the Data Protection Act 2018 and the General Data Protection Regulation (EU) 2016/679) and related regulations, codes of practice etc.

1.2 This policy describes how we will seek to maintain the confidentiality of personal and sensitive details, including commercially confidential information. The policy is supported by procedures covering requests to access personal data held by us.

2.0 CONFIDENTIALITY

2.1 All employees will sign a Confidentiality Agreement (Appendix 1) on their first day of employment with the Company.

2.2 Personal or sensitive information:

- will only be collected in accordance with policies approved by the Board of Directors, and
- will be collected and processed in accordance with all current legislation, statutory regulations and/or good practice.

2.3 Manual records will be kept secure, not accessible to unauthorised personnel**,** with access restricted to those employees who require the information in order to carry out their duties. Each employee who is permitted access to the files will be responsible for ensuring that they are left secure when they have accessed the information required. Manual files containing personal or confidential information will not be left unattended on individual desks, but will either be returned to secure storage or locked in the user's desk or filing cabinet.

2.4 Members of the general public will not be permitted access to secure areas, i.e. all office areas, unless with the prior permission of the Manager.

2.5 Computer screens will always be cleared and the user will 'log off' before leaving their office. Screens will never be left with any personal or sensitive information displayed.

2.6 Our offices will be locked whenever they are unattended.

3.0 ACCESS TO INFORMATION

3.1 We will comply with all current data legislation and related statutory regulations regarding requests from employees or service users for access to the appropriate information held about them.

3.2 A request for access to personal data will normally be accepted only if it is made in writing by the individual concerned or by a person formally authorised in writing to make the request on behalf of the individual, in accordance with the regulations.

3.3 Normally information held by Almond Enterprises Ltd about a service user or employee will not be passed on to any other agency or individual without the written permission of the person concerned. The only exception to this general rule will be where the passing on of such information is permitted by law, e.g. where a Police investigation into criminal activity requires the divulging of information held by the Company. Such a request may be accompanied by a Court Order.

3.4 We will ensure that, if required, appropriate agreements, protocols or contracts are entered into with all third parties with whom we may require to share personal or sensitive information.

We will ensure that any 'non-disclosure' clause within contracts, covering any personal data company employees may access in the course of their work, is adhered to.

3.5 We will ensure that, apart from the exceptions described below, all reports to our Board of Directors relating to individual service users or employees are 'anonymous', i.e. that the individual's name does not appear in the report.

The exceptions will be where identification is essential to the Board's consideration of the matter, e.g. in considering an appeal, or a complaint.

3.6 With the exception of 'positive' events such as an official opening, we will ensure that in making any general information available to the media or other agencies, the anonymity of service users or employees is maintained, unless written permission is obtained in advance for names to be released or individuals to be identified.

4.0 FINANCIAL AND OTHER MANAGEMENT INFORMATION

4.1 The principles described above will also apply as appropriate to all financial and general management information.

4.2 The proceedings of Board and any other Sub-Committee or Working Group meetings will be regarded by all those present as being confidential, with the approved minutes of each meeting being the publicly available record of each discussion.

5.0 USE OF INFORMATION AND BREACH OF CONFIDENTIALITY

5.1 All information held by us will only be used for the purposes for which it has been obtained. In particular, the Board of Directors and employees will not use any information obtained in the carrying out of their duties or responsibilities for personal gain, or pass any such information on to any other person who might use it in such a way.

5.2 A breach of confidentiality by a Director may result in that person having to resign from the Board. Any breach of confidentiality by an employee will result in disciplinary action.

6.0 DISPOSAL OF CONFIDENTIAL INFORMATION

6.1 We will ensure that all files and confidential papers which are no longer required are disposed of by one of the following methods:

1. by using a paper shredding machine;
2. by placing papers into the 'confidential waste' plastic bags which will be disposed of in accordance with current arrangements.

7.0 TRAINING

7.1 All employees will receive training in the operation of current data legislation at the level appropriate to their specific duties, and in the maintenance of the confidentiality and security of manual and computer information held by the Company.

7.2 The main training will be undertaken as part of the induction process for all new employees. Refresher training will be given to all employees at regular intervals as part of our ongoing learning and development programme.

8.0 IMPLEMENTATION AND REVIEW

8.1 The Manager is responsible for ensuring that all employees comply with this policy, and with all current legislation etc. relating to confidentiality of information. The Chairperson is responsible for ensuring that all Directors comply.

8.2 The Manager is the Company's Data Protection Officer.

8.3 As required, the Manager will report to the Board on the implementation of this policy, and in particular on the number of requests received for access to personal data held by the company.

8.4 The Manager will ensure that this policy is reviewed every 3 years by the Board of Directors.

FIRST APPROVED IN	**NOVEMBER 2007**
CURRENT VERSION 5.0 APPROVED IN	**MAY 2019**
NEXT REVIEW DUE BY	**MAY 2022**

Confidentiality Agreement

I undertake to respect the confidentiality of all aspects of my work, and the privacy of individuals and organisations with whom I am dealing.

I agree to be bound by the duty of confidentiality. I shall not disclose particulars of individuals, the identity of service users or the nature and extent their interests.

If it is necessary for the proper discharge of my functions to disclose information about a service user, I shall first seek permission from that service user and shall only provide such information that the service user agrees to.

Where a duty of confidentiality is owed to a third party I shall respect both this duty and the duty to the service user.

I understand that any breach of confidentiality is a disciplinary offence.

Name (please print): _____

Signed: _____

Date: _____