01 - Information Governance Policy

Version:	3
Last review date:	January 2019
Reviewed by:	Lisa Boullé, Business Support Manager
Next Review date:	January 2021
Approved by:	Anne Stenning, CFO

Contents

1. Principles

Brain-In-Hand Ltd (hereafter the Company) recognises the need for an appropriate balance between openness and confidentiality in the management and use of information.

The Board and Executive fully support the principles of corporate governance, but equally place importance on the confidentiality of, and the security arrangements to safeguard, both personal information about systems users and staff and commercially sensitive information.

The Company also recognises that where there is the need to share user information with partner organisations, it is done in a controlled manner consistent with the interests of service users.

The Company acknowledges that information is a valuable asset, therefore it is wholly in its interest to ensure that the information it holds, in whatever form, is appropriately governed, protecting the interests of all of its stakeholders.

Accurate, timely and relevant information is essential to deliver the highest quality service. It is the responsibility of all staff to:

- ensure and promote the quality of information
- actively use information in decision making processes
- safeguard the movement of personal identifiable data in the organisation.

To achieve this, the Company will operate under the following principles:

a. Openness

- Information on the Company and its services should be available to the public through a variety of media.
- Service users should have ready access to their own information and know how it is held and processed by the company.

b. Legal Compliance

- The Company regards all identifiable personal information relating to users as confidential.
- The Company will undertake annual assessments of its compliance with legal requirements.
- The Company regards all identifiable personal information relating to staff as confidential.
- The Company will establish and maintain policies to ensure compliance with the Data Protection Act and the common law confidentiality.
- The Company will establish and maintain policies for controlled and appropriate sharing of user information with partner organisations.

c. Information Security

- The Company will establish and maintain policies for the effective and secure management of its information assets and resources.
- The Company will undertake annual assessments of its information and IT security arrangements.
- The Company will promote effective confidentiality and security practice to its staff through policies, procedure, spot-checks and training.
- The Company will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.

d. Information Quality Assurance

- The Company will establish and maintain policies and procedure for information quality assurance and the effective management of records.
- The Company will undertake annual assessments of its information quality and records management arrangements.
- All managers are expected to take ownership of, and seek to improve, the quality of information with their services.
- Wherever possible, information quality should be assured at the point of collection.
- The Company will promote information quality and effective records management through policies, procedures, user manuals and training.

e. Confidential Information

- All user and client data will be treated as confidential and only released to authorised individuals under strict guidance.
- Where the company publishes amalgamated data reports or case studies, it will ensure that no user can be identified unless that user's informed, written consent is obtained.
- Access to user and staff information will be restricted to authorised staff on a need to know basis.
- A register of information assets will be maintained.
- A register of staff access authorities to the BIH system will be maintained.
- There will be physical security procedures for all data stored on site.
- All data is stored and processed on an external server we will ensure that this is (1) within the European Economic area or within an area that is covered by an EU adequacy decision (2) properly and regularly backed up and (3) preserved as fully as possible against inappropriate disclosure requirements.
- In all possible cases user consent will be obtained before any indefinable release. For example, all facilitator service users are required by our licence to sign a consent to release form in case of emergency.

2. Responsibilities

It is the role of the Executive to define the Company's policy in respect of Information Governance, taking into account legal requirements and those of partner organisations. The Board is responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

The IG Lead is responsible for overseeing day to day Information Governance issues, developing and maintaining policies, standards, procedures and guidance, co-ordinating Information Governance in the Company and raising awareness of Information Governance.

Managers within the Company are responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is continuing compliance.

All staff, whether permanent, temporary or contracted, are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring they comply with these on a day to day basis. Their responsibilities for Information Governance include maintaining confidentiality of data, ensuring secure storage of data and being aware of situations where disclosure may be required. All staff receive appropriate training in IG and Data Protection.

3. Monitoring the Policy

The IG Lead is responsible for:

- monitoring of IG policy and all procedures relating to it;
- producing and implementing an annual improvement plan;
- reporting to the Executive team;
- ensuring that any IG breaches are brought to the attention of the executive team and that appropriate remedial action is taken.