CONFIDENTIALITY AND DATA SECURITY POLICY
[May 2018]

This document sets out the policy of LA Business Recovery Limited ("the Company") on the confidentiality and security of the information which it deals with in the ordinary course of its business activities and the expectations it places upon employees, workers, contractors, volunteers and interns (collectively referred to as Staff Members) in respect of that information.

Acting lawfully and protecting the privacy of our Staff Members, prospective clients and those involved in the formal insolvency appointments that we deal with is a responsibility that the Company takes seriously at all times.

This policy applies to the confidentiality and privacy of the information that Staff Members deal with.

Confidentiality

Insolvency Practitioners as licensed professionals must observe a Code of Ethics. That Code includes the fundamental principle of confidentiality:

> *An Insolvency Practitioner should respect the confidentiality of information acquired as a result of professional and business relationships and should not disclose any such information to third parties without proper and specific authority unless there is a legal or professional right or duty to disclose. Confidential information acquired as a result of professional and business relationships should not be used for the personal advantage of the Insolvency Practitioner or third parties.*

All Staff Members are required to observe this obligation in all of their dealings for or on behalf of the Company and its insolvency practitioners.

Staff Members who are in any doubt about whether a proposed course of action would constitute a breach of the fundamental principle of confidentiality should discuss the proposed course of action with their Line Manager.

Individuals, companies, partnerships and other artificial legal persons all have rights to confidentiality that Staff Members must respect.

Confidential information and personal data

The nature of insolvency practice is such that confidential information (some of which may also be described as personal data) will come into the hands of Staff Members in the ordinary conduct of the Company's business activities. This will include circumstance such as:

- As an employer in respect of its own Staff Members;
- When advising prospective clients about their circumstances;
- When conducting formal insolvency appointments;

- When undertaking training, marketing and networking activities.

A duty of confidentiality always applies to client information. Additionally, there may be further legal obligations in respect of the various types of personal data that comes into our possession.

Data protection

Legal requirements around data protection apply to information that relates to an individual, which is identifiable to them. While companies, (such as the Company itself), may have rights to confidentiality in respect of their business information, the data protection framework relates to information about living persons (i.e. their personal data).

Examples of personal data that the Company holds include (but are not limited to) an individual's name, address, date of birth, who they worked for or how much money they are owed by someone else, depending upon which category of individual we are dealing with (e.g. debtors, creditors, employees of insolvency companies or our own employees).

A list of the different types of personal data ("data categories") that we deal with in respect of different individuals ("data subjects"), can be found in our Data Processing Register, which is available on request. Please email Virgil Levy at virgil@labr.co.uk.

The Data Protection framework provides safeguards to protect the privacy of individual's data.

More stringent requirements exist in respect of personal data that is considered to be particularly sensitive, known as special category data (see our Special Category Data Policy). These additional requirements that protect the privacy of data subjects are reflected by the Company throughout its approach to data access and security.

For each category of person that we deal with, there is a relevant Privacy Notice, which describes what personal data we may hold about them, why we consider it to be lawful for the Company to hold that data, how long we intend to hold it for and for what purpose(s) it will be used. In some instances, individuals are afforded rights to object to our processing of their data and in others they are not. Full details are set out in each of the Privacy Notices for:

- Staff Members and job applicants
- Business contacts and customers
- Debt advice and personal insolvency clients
- Directors, shareholders and owners of insolvent businesses
- Creditors, book debtors and employees of insolvent businesses (Stakeholders)

With the exception of the Staff Member and Job Applicant Privacy Notice, all privacy notices are located on our website. These documents contain details of the rights of each category of persons and when the policy should be highlighted to the individual concerned (which is typically, at the first available opportunity, or within one month of our starting to deal with their personal data).

Individuals have legal rights that their personal data is processed fairly and in a way that protects their privacy. Staff Members are required to adhere to the terms of this and other relevant policies in order not to breach those rights.

Ensuring confidentiality and data privacy

This policy sets out the practical measures and internal processes that the Company has put in place to ensure confidentiality and data privacy.

The Company's responsibilities

The Company will be responsible for ensuring that:

- Its servers are secure from unauthorised access by third parties by use of appropriate firewall protection, taking into account the advice of its IT service providers;
- Server backup procedures are in place and implemented consistently to a secure cloud location which meets prevailing EU data protection standards;
- Its business premises are secure when unoccupied;
- All equipment that it provides for use in connection with its business will be security marked or tagged for the purpose of tracking and where such security tagging is undertaken, the equipment will be suitably marked;
- All obsolete equipment is properly and securely disposed of;
- Anti-virus and anti-malware software is kept up to date on the equipment that it supplies to Staff Members (with Staff Members required to make that equipment available for update, immediately upon request);
- Staff Members receive training and support in complying with this policy and other relevant policies as pertain to confidential information or personal data.

Protection of computer equipment from loss, theft or unauthorised access

Staff Members are responsible for ensuring that all computers and other portable devices such as smartphones, tablets and laptops (collectively referred to as computer equipment) that may contain

or provide access to confidential information or personal data are protected from loss, theft and unauthorised access, in accordance with this policy.

Practical steps to ensure the protection of computer equipment and the confidential information and personal data that it may contain or be used to access, include:

- Not removing computer equipment belonging to the Company from the Company's office without prior approval;

- Taking reasonable care to ensure the physical security of computer equipment, for example by:

    - Never leaving equipment unattended in a public place, at any time (e.g. such as when visiting comfort facilities on a train or in a café);

    - When leaving equipment unattended in a private place (such as your home), ensuring that it is not left in an insecure location (e.g. by locking your premises when they will be unattended);

    - Never leaving computer equipment on view in an unattended vehicle. Always ensure that such equipment is locked in the boot, out of sight;

- Taking reasonable care to ensure that the confidential information or personal data is not subject to unauthorised access by:

    - Use of an agreed security mechanism, appropriate to the capabilities of the device (e.g. passwords, pin numbers, finger print or iris recognition), to prevent unauthorised access;

    - Changing passwords or pin numbers on a regular basis, and at a minimum, every 3 months;

    - Ensuring passwords and pin numbers are not easily identifiable (e.g. dates of birth, names of family members or pets). Passwords should include a mixture of upper and lower-case text and numbers and be a minimum of 8 characters in length, pin numbers should be a random sequence of not less than 6 characters in length;

    - Not disclosing passwords or pin numbers to any other person, except to the Company's Directors, (who will securely maintain a list of all security measures that are applied to the Company's equipment) or upon the express instruction of an Executive Director of the Company.

    - Not allowing other persons (such as children or family members) to use the Company's equipment, even when they are trusted by you.

- Accessing data via a secure link to the Company's central servers, wherever this is possible.

- Minimising the creation of local copies of confidential information and/or personal data.

- Not leaving equipment while logged into your account and visible to third parties (authorised or otherwise), when equipment is not in use;

- Not transmitting information that may be confidential and/or contain personal data over public or insecure networks. Communications should be drafted and sent when a secure connection is available;

- Never including information that may be confidential and/or contain personal data within the body of an unencrypted email. Instead confidential or personal data should be contained either in encrypted communications or in a password-protected format as an attachment to an email;

- Advising the prospective recipients of confidential and/or private data of any password that is required for the purposes of access within a separate communication to them;

Protection of hard copy documents

Hard copy documents belonging to the Company or its clients are to be maintained at Company controlled premises. Staff Members should only remove hard copy documents from Company controlled premises with appropriate permission, in accordance with the Company's *Off-Site Working Policy* and when it is necessary for the Company's business activities for them to do so. This policy is available on request via virgil@labr.co.uk or to Virgil Levy in writing.

Where hard copy documents are required to be removed from Company controlled premises (for instance, while homeworking), they should be retained for only so long as is necessary and returned to the Company's premises as soon as is reasonable practicable.

Practical steps to ensure the protection of hard copy documents and the confidential information and personal data they may contain, include:

- Taking reasonable care to ensure the physical security of documents, in a similar manner to computer equipment;

- Maintaining a tidy working environment ("clear desk") in order that documents are not viewed by unauthorised persons;

- Minimising unnecessary duplication of documents and secure destruction of unneeded copies.

Non-disclosure of confidential information or personal data to third parties

Staff Members should not disclose confidential information and/or personal data about the Company, colleagues or third parties unless that disclosure is fair and lawful. Doing so may constitute a breach of the duty of confidentiality and/or the data subject's privacy.

To protect against a breach of confidentiality or data privacy:

- Staff Members must not make any oral or written reference to personal data held by the Company about any individual except to Staff Members of the Company who need the information for their work or an authorised recipient.

- Care should be taken to establish the identity of any person asking for access to confidential information and/or personal data to make sure that the person is entitled to receive the information.

- If a Staff Member is asked by an unauthorised individual to provide details of personal information held by the Company the Staff Member should ask the individual to put their request in writing and send it to the Case Supervisor. If the request is in writing the Staff Member should pass it immediately to their Line Manager.

The rights of data subjects to access the personal data that the Company processes about them are described in the relevant *Privacy Notices* and within the Company's Data Subject Access Policy. The subject themselves may be authorised recipients, in accordance with that policy. This policy is available on request via virgil@labr.co.uk or to Virgil Levy in writing.

Staff Member's responsibilities

- Staff Members must take confidentiality and security seriously, whether the Staff Member considers the information to be sensitive or not.

- If a Staff Member is in doubt about any matter to do with confidentiality or data privacy they must refer the matter to their Line Manager immediately.

- Staff Members must not use confidential or personal information for any purpose other than their work for the Company.

- Staff Members must diligently observe any instruction or guidelines issued by the Company in relation to confidentiality and data protection.

- In the event that a Staff Member becomes aware of any breach of this policy, they must report it in accordance with the Company's Data Breach Policy.

- Any failure to follow the procedures and guidance laid out in this Policy may lead to disciplinary action which could result in termination of employment.

- The Company reserves the right to pursue a claim for recovery of costs incurred where an employee fails to adhere to this Policy and the Company suffers loss or damage.