Beesley Corporate Recovery Limited

Data Protection Policy January 2020

Our Approach to Data Protection and Information Management

This policy sets out the firm's approach to data protection and information management, including how the firm manages confidential information and the precautions the firm takes to keep information secure.

The person responsible for this policy Mike Davies. The policy is reviewed and updated annually.

Protection & Security of the Information Assets

The great majority of the information assets are confidential. We take care to protect confidential information applying the principles set out in this policy.

This policy will be periodically circulated to all staff to remind them of their responsibilities.

Retention & Disposal of Information

We retain information for the periods required. These periods reflect our data protection obligations not to keep personal data for longer than is necessary, and also our statutory, regulatory and business needs to keep records.

Thereafter information is disposed of securely, by shredding, electronic deletion, or otherwise as appropriate.

Firewalls

The firm maintains a firewall to prevent unauthorised access to the firm's network and data.

Procedures to Manage User Accounts

User accounts are managed by our IT Department and user accounts can be disabled at any time, for example on discovering a breach of security. Accounts are disabled when an employee leaves the firm.

Employees responsible for the management of payments (including fee earners and finance staff) are only recruited or assigned to that function after passing suitable background checks, including taking references and the verification of claimed qualifications.

Procedures to Detect and Remove Malicious Software.

If, despite the precautions described elsewhere malicious software (malware) is present on the system this should be detected by the firm's anti-virus software. It is then the responsibility of the firm's IT department to remove the malware, according to the nature of the threat and industry standard procedures at the relevant time.

Employees are advised that, without the consent of the Compliance Officer, no additional software is to be downloaded or used on this firms' systems.

Training for Personnel on Information Security

The Firm has provided all employees with its information security rules (the current version of which is set out below) and recirculates them to all staff on an annual basis.

In addition, the firm trains employees about information security risks and precautions on induction, and thereafter on an annual basis. In addition, the Compliance Officer will also periodically circulate emails and training information reminding employees of their duties and current criminal methodologies and risks, as well as necessary precautions.

Updating and Monitoring of Software

All software used by the firm is supported by external software suppliers who issue routine updates from time to time. It is the responsibility of the Compliance officer/IT Manager to decide whether and when updated versions are to be installed or the new or better software should be obtained.

Part B

Data Protection & Information Management – Employee Responsibilities

Who is Responsible

The firm holds a large amount of confidential information about clients, staff and third parties. We must all ensure that all employees comply with data protection law and ensure that confidential information is kept secure. Accordingly all employees must study and observe the precautions set out below.

The firms Compliance Officer has overall responsibility for data protection and this policy. Questions or concerns about these issues should be referred to your line manager in the first instance.

In particular if you are aware of any breaches of security with confidential information you must report that breach immediately to that person. The firm has a duty to report breaches of security to clients, and in certain cases to the information Commissioners Office.

Our Obligations

When we hold information about identifiable people (known as “data subjects”) this gives rise to obligations under the General Data Protection Regulation (GDPR). The GDPR applies whether such information is held in electronic form or in a paper filing system.

People have rights, if we hold information about them. That includes the right to be informed what we hold, the right to have errors corrected and the right to have data deleted if we have no justification for holding it.

We may be liable in various ways if we fail to hold data appropriately. This may include liability in damages for negligence and breach of confidentiality or even criminal liability. We may also be subject to professional sanctions for breach of the ACCA and Insolvency Service code of conduct.

The Data Protection Principles: In processing personal data we must be able to demonstrate that we comply with the “data protection principles”. These require that personal data must be:

Processed lawfully, fairly and in a transparent manner

Collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.

Adequate, relevant and limited to what is necessary

Accurate and, where necessary, kept up to date

Kept for no longer than is necessary

Kept with appropriate security

Grounds for processing personal data

We should only process personal data if we have a legitimate justification for doing so.

Often the justification will be the consent of the person concerned, however, in the instance where some one can not provide consent, e.g. they are under the age of 16, or have provided written consent for a third party to act on their behalf, consent is required from the person holding responsibility.

Otherwise we will be entitled to proceed without consent on a number of grounds. Those which most often apply are the following:

It is necessary for the performance of a contract to which the person concerned is a party

It is necessary for compliance with a legal and/or statutory obligation

It is necessary to protect someone's vital interests

It is necessary for our legitimate interests or those of a third party, except where such interests are overridden by the interests or rights of the person concerned.

Sensitive Personal Data

Sensitive personal data (Referred to the GDPR as "Special Categories of personal data") can only be processed under strict conditions. Sensitive personal data includes information about someone's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life and sexual orientation, genetic data and biometric data.

The usual grounds which entitle us to process such sensitive data are the following:

Explicit consent of the data subject

It is necessary to protect the vital interests of data subject who is physically or legally incapable of giving consent.

Data manifestly made public by the data subject

It is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.

Your Responsibilities

Do not collect or use personal data without a good reason

If clients give us information about themselves this is rarely a problem, as they will usually expect us to record that information and use it for our usual professional purposes.

However, we should take particular care with information about third parties, who may be unaware that we hold information on them. We are required to bear in mind three simple principles:

Do not record information about people unless you need to do so

Keep all information secure

Delete information promptly when no longer required

Those principles apply especially to information of an embarrassing, secret or sensitive nature, and where the people concerned have not consented to us holding the information.

Take care when sending personal data to others

We will often find the need to share personal data and confidential information with others such as, agents, solicitors, accountants etc. however before doing so we need to consider these issues:

Do they really require the information?

Should we redact documents so that they do not include irrelevant and unnecessary confidential information.

Can we rely upon the recipient to keep the information secure?

Are we sending the information outside the European Economic Area? If so we need to check that the country in question has been designated by the EU Commission as providing adequate data protection, or that we have appropriate contract clauses agrees with the recipient place to protect data.

In publications and publicity material all client identification information must be removed unless clients have consented.

Keep Papers Secure

Keep confidential papers in locked cabinets, when they are not in use. Bear in mind that cleaning personnel, temporary staff and others may be present in the building and that leaving papers where they can be seen risks a breach of security. A clear desk policy must be maintained to ensure this when you are not in the office.

Report any strangers you see in entry-controlled areas.

Only take client files (or other confidential information) out of the office when it is necessary to do so. Take precautions to ensure that such items are not stolen or lost.

Be aware that taking paper files out of the office is especially risky, where possible take in an encrypted digital form

Ensure confidential papers are shredded on disposal in line with firm and regulatory policy

Keep IT Secure

Take care with any email you receive from an unknown source. Remember that, clicking on attachments or links may result in viruses being downloaded.

Follow the firm's policy on the use of passwords, including the level of complexity, the frequency with which they should be changed, and the other precautions such as not writing them down in any form which might be intelligible to a third party. Secure passwords are particularly important with mobile devices, or with logins that would enable people to access the firm's systems remotely.

Log off from your computer when it is left unattended or ensure that it is locked.

Ensure that your computer screen does not show confidential information to those who are not authorised to see it. This is particularly important when using a laptop or other device outside of the office.

Update the software on your computer whenever required to do so.

Take particular care when transferring data between the firm's systems and an external system: e.g.

If you transfer data using a data stick or similar storage device.

If you transfer files to a home computer you must ensure that your computer is properly secure. That is a particular risk if your home computer is shared with other users or vulnerable to theft.

Even if data has been deleted from electronic media it may be possible for others to recover it. All computer hard drives, data sticks, floppy disks, CDs etc should be cleaned professionally or physically destroyed when no longer required.

Take care with payments

The firm has policies in place to protect itself from the risk of funds being diverted. Those responsible for making payments from our bank accounts receive separate guidance, which includes strict prohibition on divulging account credentials or security information (including usernames, passwords, PIN Numbers and other security codes).

All employees should be aware of the risk of criminals seeking to divert funds, e.g. by phone calls, emails to the firm purporting to be from clients, banks, or to clients purporting to be from the firm, asking for payments to be made to inappropriate accounts. Employees must immediately report to their manager or the compliance officer immediately any request they receive for information which might be used to facilitate fraudulent payments.

Take care when dealing with enquires

Beware of "blaggers", (people who attempt to obtain confidential information by deception). This is most commonly done by phone but may also be by email or in person. The following precautions should be taken:

Check the identity of the person making the enquiry

Check we are authorised by the client (or authorised person), to pass the information on.

Ask the enquirer to put their request down in writing – if made in person or by phone.

Refer to your manager if you are unsure

Take particular care with callers who claim to be from our bank.

Forward any "subject access request" you receive

Under the GDPR we may receive a written request (known as a subject access request) from someone for information that we hold about them. If a request is received this should be forwarded to the compliance officer immediately.