jdm Data Protection Policy

WARNING

Failure to comply with the firm's policies, as set out in this manual, may be treated as gross misconduct and result in disciplinary action.

This policy sets out the firm's approach to data protection and information management, including how the firm manages confidential information and the precautions we take to keep information secure. It has been approved by the Senior Management of the firm. It supplements the training with which you have also been provided. It is important that you read this manual, and refer to it when relevant issues arise.

Our Data Protection Officer is Elisabeth Howard. Consult her in cases of difficulty. In her absence, consult the Deputy Data Protection Officer, who is Mark Burgess.

1. Who is Responsible?

The firm holds a huge amount of confidential information about people including clients, other parties to transactions, and staff. We must all comply with data protection law and keep confidential information secure. Accordingly all staff must study and observe the precautions set out below.

The Data Protection Officer has overall responsibility for data protection and this policy. Questions on or concerns about these issues should be referred either to her or to your supervisor.

In particular if you are aware of breaches of security with confidential information you must report that promptly to that person. The firm has a duty to report breaches of security to clients, and sometimes to the Information Commissioner's office.

2. jdm's 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. The following is a summary of our obligations under data protection law, but is not a substitute for research where appropriate.

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 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. Otherwise we may 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 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 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 sensitive personal data are the following:

- Explicit consent of the data subject.
- It is necessary to protect the vital interests of a 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.

3. 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 the usual purposes of our business. However take particular care

with information about third parties, who may be unaware that we hold information about them. Bear in mind three simple principles:

- **Do not record information about people unless you need to do so.**
- **Keep it secure.**
- **Delete it promptly when it is 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.

You will often need to share personal data and confidential information with others such as solicitors, counterparties to transactions, surveyors and others. However before doing so consider these issues:

- Do they really need the information?
- Should we redact documents so that they do not include irrelevant and unnecessary confidential information?
- Can we rely on the recipient to keep the information secure?
- Also, take extra care before sending personal data outside the European Economic Area. Before doing so you should check either that the country in question has been designated by the EU Commission as providing adequate data protection, or that we have appropriate contract clauses agreed with the recipient to protect the data.

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.

- Report any stranger you see in an entry-controlled area.
- Only take confidential files out of the office when it is necessary to do so. Take precautions to ensure that such items are not stolen or lost. For example do not leave files in an unattended car.
- Be aware that taking paper files out of the office is especially risky. Where possible take information in encrypted digital form, e.g. on a laptop.
- Also bear in mind that laptops and other electronic devices may be stolen if taken out of the office. Hence confidential files taken out of the office in electronic form must be encrypted. It is not enough that the machine on which they are stored is password protected. Where possible if you are working out of the office, access documents over the internet.
- Ensure confidential papers or papers containing personal data are shredded on disposal.

Keep IT secure

- Take care with any e-mail you receive from an unknown source. Bear in mind 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 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.

- 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 the office.
- Update the software on your computer whenever required to do so. Updates frequently fix security weaknesses.
- Take particular care when transferring data between the firm's system and an external system. For example:
- if you use a data stick or similar storage device to load documents onto your work computer that may introduce viruses or other malware into the firm;
- Even if data has been deleted from electronic media it may be possible for others to recover it. Hence computer hard drives, data sticks, floppy disks, CD-ROMs etc should either be cleaned by an expert 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 account receive separate guidance, which includes a strict prohibition on divulging account credentials or security information (including usernames, passwords, PINs and other security codes).
- All staff should be aware of the risk of criminals seeking to divert funds, e.g. by phone calls or e-mails to the firm purporting to be from clients, our bank or senior staff, or to clients purporting to be from the firm, asking for payments to be made to inappropriate accounts. Staff must report to their supervisor or Elisabeth Howard immediately any request they receive for information which might be used to facilitate fraudulent payments.
- If taking credit cards payments credit card details must never be recorded/written anywhere and credit card details should only ever be taken over the telephone and not sent by email. Please make sure credit card details are not provided on a telephone call which is put through by Rightmove as these calls are recorded. Any payments must be processed while the client is on the telephone call, not processed at a later date.

Take Care When Dealing with Enquiries

- Beware of "blaggers" (people who attempt to obtain confidential information by deception). This is most commonly done by phone but may also be by e-mail or by calling in person.

The following are examples of the precautions you should take when dealing with enquiries.

- Check the identity of the person making the enquiry.
- Check we are authorised by the client or other relevant person to pass on this information.
- Ask callers to put their request in writing if you are not sure about the caller's identity and their identity cannot be checked.
- Refer to your supervisor for assistance in difficult situations.
- Take particular care with callers who claim to be from our bank. Some firms have had money stolen from their bank accounts after staff gave confidential banking information out over the phone.
- Under data protection law we may receive a written request (known as a "subject access request") from someone for information that we hold about them. If you receive such a request you should forward it to Elisabeth Howard immediately.

Protection and Security of Confidential Information

Confidential information will not be passed to anyone outside the firm other than with the consent of the client (where appropriate) or where client confidentiality does not apply, when that is reasonably necessary for normal business purposes. In publications and publicity material all client identification information will be remove.

Retention and Disposal of Information

We retain information for the periods set out in the Information Asset Register. These periods reflect our data protection obligation 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

Each branch maintains its own Firewall to prevent unauthorised access to the firm's network and data. All messages entering or leaving the firm's intranet pass through the Firewall, which blocks those that do not meet specified security criteria by applying a rule set which establishes a barrier between the trusted secure internal network and the internet or other networks which are not assumed to be secure or trusted. There is also a Firewall at the Datacentre where the main Domain Controller is held. This Firewall is completely locked down and only allows Safe Data Storage to access to it. This Firewall only accepts emails from Symantec Messagelabs, which is the external malware scanner and this Firewall also has a VPN connection to all branch Firewalls, meaning everyone can access emails and network drives securely in the branch. All jdm PCs also have Windows Firewall turned on.

Antivirus

All PCs and servers are protected using Symantec Endpoint Protection, which is managed and installed from the Manager console installed on the Domain controller. From here, updates will be pushed out once Symantec release them. So all PCs are then protected from zero day threats.

Symantec Mail Security for Microsoft Exchange (SMSMSE) – this piece of software scans all incoming and outgoing Mail ports for potential Malware and other malicious items inside emails. This software is internal and scans emails once they enter or exit the Exchange server.

Symantec Messagelabs – This is the external mail scan software. This will check and if required block spam and malicious emails before they are able to get to the Exchange system. We have also locked down the Firewall and Exchange server to only receive emails from Symantec's specified servers, meaning bad emails can't bypass this system and get through.

Secure Configuration of Network Devices

The firm uses a standard Local Area Network provided by Safe Data Storage, which provides appropriate security configuration. Every user has explicit credentials to log into their accounts and folders have set permissions on them preventing unauthorised access when required.

Procedures to Manage User Accounts

User accounts are managed by Nicola Bellward and Lizzy Howard. User accounts can be disabled at any time, for example on discovering a breach of security. Accounts are disabled when a member of staff leaves the firm.

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 authorised third party supplier, Safe Data Storage to remove the malware, according to the nature of the threat and industry standard procedures at the relevant time.

Register of Software Used by the Firm

The firm currently uses the following software:

- 1x Windows Small Business Server 2011
- 1x Microsoft Exchange 2010
- 1x Windows Server 2012 R2 Standard
- 3x Windows Server 2008 Standard
- 3x VMware on Severs
- Exclaimer Signature Manager Exchange Edition
- Mixture of Office 2010/2013/2016 on all PC's
- StorageCraft Backup software on all server (ShadowProtect, ImageManager)
- 3x SDSL Cloud Backup Client on servers.
- 1x Symantec Endpoint Protection Manager
- 45x Symantec Endpoint Protection in use.
- 1x Symantec Mail Security for Microsoft Exchange

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 Safe Data Storage to decide whether and when updated versions are to be installed or new or better software should be obtained.