Policy—Information Security – Sarfraz & Naydenov Solicitors

1 Introduction

1.1 Sarfraz & Naydenov Solicitors Ltd is committed to the highest standards of information security and treats confidentiality and data security extremely seriously.

1.2 In relation to personal data, under Retained Regulation (EU) 2016/679, UK General Data Protection Regulation (UK GDPR), the Company must:

1.2.1 use technical or organisational measures to ensure personal data is kept secure, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage;

1.2.2 implement appropriate technical and organisational measures to demonstrate that it has considered and integrated data compliance measures into the Company's data processing activities; and

1.2.3 be able to demonstrate that it has used or implemented such measures.

1.3 This purpose of this policy is to:

1.3.1 protect against potential breaches of confidentiality;

1.3.2 ensure all our data assets and IT facilities are protected against damage, loss or misuse;

1.3.3 support the Company's data protection policy in ensuring all staff are aware of and comply with UK law and the Company's procedures applying to the processing of personal data; and

1.3.4 increase awareness and understanding in the Company of the requirements of information security and the responsibility of staff to protect the confidentiality and integrity of the data that they themselves handle.

2 Definitions

For the purposes of this Policy:

business information	means business-related information other than personal information regarding customers, clients, suppliers and other business contacts of the Company;
confidential information	means trade secrets or other confidential information (either belonging to the Company or to third parties) that is processed by the Company;
personal data	(sometimes known as personal information) means data relating to an individual who can be identified (directly or indirectly) from that data;
pseudonymised	means the process by which personal data is processed in such a way that it cannot be

	used to identify an individual without the use of additional data, which is kept separately and subject to technical and organisational measures to ensure that the personal data cannot be attributed to an identifiable individual;
special category data	(formerly 'sensitive personal data') means personal data about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetic data, biometric data (where used to identify an individual) and data concerning an individual's health, sex life or sexual orientation.

3 Roles and responsibilities

3.1 Information security is the responsibility of all staff. Muhammad Sarfraz is in particular responsible for:

3.1.1 monitoring and implementing this policy;

3.1.2 monitoring potential and actual security breaches;

3.1.3 ensuring that staff are aware of their responsibilities; and

3.1.4 ensuring compliance with the requirements of Retained Regulation (EU) 2016/679, UK GDPR and other relevant legislation and guidance.

4 Scope

4.1 The information covered by this policy includes all written, spoken and electronic information held, used or transmitted by or on behalf of the Company, in whatever media. This includes information held on computer systems, hand-held devices, phones, paper records, and information transmitted orally.

4.2 This policy applies to all staff, including employees, temporary and agency workers, other contractors, interns, volunteers and apprentices.

4.3 All staff, Paralegal, Solicitors or Fee Earners must be familiar with this policy and comply with its terms.

4.4 The Company information covered by this policy may include:

4.4.1 personal data relating to staff, customers, clients, suppliers;

4.4.2 other business information; and

4.4.3 confidential information.

4.5 This policy supplements the Company's Data Privacy Policy which can be found on our website, Client Care Letter, and other policies and privacy notices relating to relevant

policies, eg internet, email and communications, document retention and the contents of those policies must be taken into account, as well as this policy.

4.6 We will review and update this policy regularly in accordance with our data protection and other obligations. It does not form part of any employee's contract of employment and we may amend, update or supplement it from time to time. We will circulate any new or modified policy when it is adopted.

5 General principles

5.1 All Company information must be treated as commercially valuable and protected from loss, theft, misuse or inappropriate access or disclosure.

5.2 Personal data, and special category data, must be protected against unauthorised and/or unlawful processing and against accidental loss, destruction or damage, by the use of appropriate technical and organisational measures.

5.3 Staff should discuss with line managers the appropriate security arrangements and technical and organisational measures which are appropriate and in place for the type of information they access in the course of their work.

5.4 Company information (other than personal data) is owned by the Company and not by any individual or team.

5.5 Company information must be used only in connection with work being carried out for the Company and not for other commercial or personal purposes;

5.6 Personal data must be used only for the specified, explicit and legitimate purposes for which it is collected.

6 Information management

6.1 Personal data must be processed in accordance with:

6.1.1 the data protection principles, set out in the Company's data protection policy;

6.1.2 the Company's data protection policy generally; and

6.1.3 all other relevant policies.

6.2 In addition, all information collected, used and stored by the Company must be:

6.2.1 adequate, relevant and limited to what is necessary for the relevant purposes;

6.2.2 kept accurate and up to date;

6.3 The Company will take appropriate technical and organisational measures to ensure that personal data is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage, including:

6.3.1 pseudonymisation of personal data;

6.3.2 encryption of personal data;

6.4 Personal data and confidential information will be kept for no longer than is necessary and stored and destroyed in accordance with the Company's *records retention policy*. Further details can be found in our client care letter when our client instructs us.

7 Human resources information

7.1 Given the internal confidentiality of personnel files, access to such information is limited to Fee Earners, Solicitors or Paralegals working in on a relevant matter. Except as provided in individual roles, other staff are not authorised to access that information.

7.2 Any staff member in a management or supervisory role or involved in recruitment must keep personnel information strictly confidential.

7.3 Staff may ask to see their personnel files and any other personal data in accordance with Retained Regulation (EU) 2016/679, UK GDPR and other relevant legislation. For further information, see the Company's *data subject access request policy*.

8 Access to offices and information

8.1 Office doors, and keys must be kept secure at all times and keys must not be given or disclosed to any third party at any time.

8.2 Documents containing confidential information and equipment displaying confidential information should be positioned in a way to avoid them being viewed by people passing by, eg through office windows.

8.3 Visitors must be required to sign in at reception, accompanied at all times and never left alone in areas where they could have access to confidential information.

8.4 Wherever possible, visitors should be seen in meeting room. If it is necessary for a member of staff to meet with visitors in an office or other room which contains Company information, then steps should be taken to ensure that no confidential information is visible.

8.5 At the end of each day, or when desks are unoccupied, all paper documents, backup systems and devices containing confidential information must be securely locked away.

9 Computers and IT

9.1 Password protection and encryption must be used where available on Company systems in order to maintain confidentiality.

9.2 Computers and other electronic devices must be password protected and those passwords must be changed on a regular basis. Passwords must not be written down or given to others.

9.3 Computers and other electronic devices must be locked when not in use and when you leave your desk, to minimise the risk of accidental loss or disclosure.

9.4 Confidential information must not be copied onto floppy disk, removable hard drive, CD or DVD or memory stick/ thumb drive without the express permission of the Mohammad Sarfraz, Director, and must be encrypted. Data held on any of these devices should be transferred to the Company's computer network as soon as possible in order for it to be backed up and then deleted from the device.

9.5 All electronic data must be securely backed up at the end of each working day. This happens automatically for all data stored on the our Company's computer network.

9.6 Staff must ensure they do not introduce viruses or malicious code on to Company systems. Software must not be installed or downloaded from the internet without it first being virus checked. Staff should contact Muhammad Sarfraz for guidance on appropriate steps to be taken to ensure compliance.

10 Communications and transfer of information

10.1 Staff must be careful about maintaining confidentiality when speaking in public places, eg when speaking on a mobile telephone.

10.2 Confidential information must be marked 'confidential' and circulated only to those who need to know the information in the course of their work for the Company.

10.3 Confidential information must not be removed from the Company's offices unless required for authorised business purposes, and then only in accordance with paragraph 10.4 below.

10.4 Where confidential information is permitted to be removed from the Company's offices, all reasonable steps must be taken to ensure that the integrity of the information and confidentiality are maintained. Staff, Fee Earners, Solicitors or Paralegals must ensure that confidential information is:

10.4.1 stored on an encrypted device with strong password protection, which is kept locked when not in use;

10.4.2 when in paper copy, not transported in see-through or other unsecured bags or cases;

10.4.3 not read in public places (eg waiting rooms, cafes, trains); and

10.4.4 not left unattended or in any place where it is at risk (eg in conference rooms, car boots, cafes).

10.5 Postal, document exchange (DX) and email addresses and numbers should be checked and verified before information is sent to them. Particular care should be taken with email addresses where auto-complete features may have inserted incorrect addresses.

10.6 All sensitive or particularly confidential information should be encrypted before being sent by email, or be sent by tracked DX or recorded delivery.

11 Personal email and cloud storage accounts

11.1 Personal email accounts, such as yahoo, google or hotmail and cloud storage services, such as dropbox, icloud and onedrive are vulnerable to hacking. They do not provide the same level of security as the services provided by our own IT systems.

11.2 Do not use a personal email account or cloud storage account for work purposes.

11.3 If you need to transfer a large amount of data, contact Muhammad Sarfraz for help.

12 Home working

12.1 Staff must not take Company information home unless required for authorised business purposes, and then only in accordance with paragraph 12.2 below.

12.2 We don't permit Staff, Fee Earners, Paralegals or Solicitors to take any information to their homes. Where staff are permitted to take Company information home, staff must ensure that appropriate technical and practical measures are in place within the home to maintain the continued security and confidentiality of that information. In particular:

12.2.1 personal data and confidential information must be kept in a secure and locked environment where it cannot be accessed by family members or visitors; and

12.2.2 all personal data and confidential information must be retained and disposed of in accordance with paragraph 6.4 above.

12.3 Staff must not store confidential information on their home computers (PCs, laptops or tablets).

12.4 You should ask Muhammad Sarfraz for the Company's homeworking policy *for* further information.

13 Transfer to third parties

13.1 Third parties should be used to process Company information only in circumstances where appropriate written agreements are in place ensuring that those service providers offer appropriate confidentiality, information security and data protection undertakings. Consideration must be given to whether the third parties will be processors for the purposes of Retained Regulation (EU) 2016/679, UK GDPR.

13.2 Staff involved in setting up new arrangements with third parties or altering existing arrangements should consult Muhammad Sarfraz, Director for more information.

14 Overseas transfer

14.1 There are restrictions on international transfers of personal data and transfers to international organisations. Staff, Paralegals, Solicitors, and Fee Earners must not transfer personal data outside the UK or to international organisations.

14.2 You should refer to the Company's data protection polic*y* for further information on international transfers.

15 Training

15.1 All staff will receive training on this policy. New joiners will receive training as part of the induction process. Further training will be provided at least every *two years* or whenever there is a substantial change in the law or our policy and procedure.

15.2 Training is provided in person.

15.3 Completion of training is compulsory.

15.4 Muhammad Sarfraz will continually monitor training needs but if you feel that you need further training on any aspect of the relevant law or our Information management and security policy or procedures, please contact him.

16 Reporting breaches

16.1 All members of staff have an obligation to report actual or potential data protection compliance failures. This allows the Company to:

16.1.1 investigate the failure and take remedial steps if necessary;

16.1.2 maintain a register of compliance failures; and

16.1.3 make any applicable notifications.

16.2 Please refer to our Personal data breach plan for our reporting procedure.

17 Consequences of failing to comply with this policy

17.1 The Company takes compliance with this policy very seriously. Failure to comply with it puts both staff and the Company at significant risk. The importance of this policy means that failure to comply with any requirement of it may lead to disciplinary action, which may result in dismissal.

17.2 Staff with any questions or concerns about anything in this policy should not hesitate to contact Muhammad Sarfraz.