This template ‘Information management and security policy’ contains suggested procedures to protect against the potential breaches of confidentiality and failures of integrity or availability of information, ensure all your information assets and IT facilities are protected against damage, loss or misuse, support our Data protection policy in ensuring all staff are aware of and comply with UK law and your own procedures applying to the processing of data, and increase awareness and understanding in the firm of the requirements of information security and the responsibility of staff to protect the confidentiality and integrity of the information that they themselves handle.

Information management and security policy

Lilac highlighted text is used to prompts users to choose one of the wording options, as appropriate.

Red highlighted text is an ‘optional’ tag.  Users can choose whether to include the wording or delete it.

Green highlighted text is an ‘insert’ tag prompting users to insert their own information (sometimes we may suggest some options to be included).

***This template is produced in partnership with Lexis®PSL Practice Compliance.***

*Lexis®PSL Practice Compliance is an online service designed to make risk and compliance easier to manage, whatever the size of your firm.   It comes with everything you need to get your compliance house in order and keep it that way, including an unbeatable range of practical guidance, templates, flowcharts, checklists and other time-saving tools.*

*See more at* <https://www.lexisnexis.com/uk/lexispsl/practicecompliance/home>*.*

Information management and security policy

Introduction

1.1 We are committed to the highest standards of document and information management and security and treat confidentiality and data security extremely seriously.

1.2 We take seriously our obligations under the Data Protection Act 1998 and all other relevant regulation and legislation.

1.3 This policy has been prepared after a detailed information asset audit[[1]](#footnote-1) and risk assessment[[2]](#footnote-2).

1.4 The purpose of this policy is to:

1.4.1 protect against the potential breaches of confidentiality and failures of integrity or availability of information

1.4.2 ensure all our information assets and IT facilities are protected against damage, loss or misuse

1.4.3 support our Data protection policy in ensuring all staff are aware of and comply with UK law and our own procedures applying to the processing of data

1.4.4 increase awareness and understanding in the firm of the requirements of information security and the responsibility of staff to protect the confidentiality and integrity of the information that they themselves handle

Responsibility

2.1 The [board OR COLP OR risk and compliance department] has overall responsibility for information management and security issues in the firm.

2.2 Every member of staff is responsible for ensuring that information held is accurate and kept confidential and that the terms of this policy are adhered to.

2.3 In the event of a data security breach, [*insert name*] must be informed immediately. See further Reporting breaches below.

2.4 The [board OR COLP OR risk and compliance department] will review security event logs and error logs on a monthly basis and are responsible for downloading and installing any necessary software or system updates.

2.5 The [board OR COLP OR risk and compliance department] will review this policy and undertake an information asset audit and risk assessment at least annually to ensure this policy remains fit for purpose and compliant with the applicable legislation.

Legal responsibilities

3.1 Our obligations under the SRA Code of Practice 2011 include that we keep the affairs of clients confidential unless disclosure is required or permitted by law or the client consents.

3.2 Our obligations under the Data Protection Act 1998 include that:

3.2.1 we only hold data with consent (or as otherwise defined in that Act)

3.2.2 we keep that data confidential

3.2.3 we use it only for authorised purpose(s)

3.2.4 any data we hold is:

(a) adequate

(b) relevant

(c) not excessive

(d) accurate, and

(e) up-to-date

3.2.5 we do not hold it for longer than is necessary

Our procedures

Information management

4.1.1 Records and information are owned by the firm and not by any individual or team.

4.1.2 Keeping accurate and up-to-date records is an integral part of all business activities.

4.1.3 Complete and accurate records must be securely stored in the appropriate locations and be easily identifiable and accessible to those who need to see them (see our separate Version control and document management policy). This means that:

(a) files must be kept in accordance with our normal file management protocols and must be kept organised and up-to-date

(b) substantive matter related emails must be placed on file and must not be stored solely in personal mailboxes

(c) files must not be removed from the office except as permitted under this policy

4.1.4 Information will be held only as long as is required, and disposed of in accordance with our Information retention and destruction policy.

4.1.5 All staff must ensure that any information and data gathered is accurate and, where appropriate, kept up-to-date. Client information must be kept on clearly identifiable client files and references using both the client’s name and our file referencing system.

Human resources information

4.2.1 Given the internal confidentiality of personnel files, access to such information is limited to the [partners OR practice manager OR HR department OR [*other*]]. Except as provided in individual roles, no other staff are authorised to access that information.

4.2.2 Any staff member in a management or supervisory role must keep personnel information confidential.

4.2.3 Subject to the provisions of the Data Protection Act 1998 and associated Codes of Conduct, staff may ask to see their personnel files at any time. See our separate Data protection policy.

Access to offices and files

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

4.3.2 All office access doors must be kept secure at all times and clients and visitors must not be given keys or pass-codes.

4.3.3 Clients should be seen in interview rooms. If it becomes necessary for you to see clients in your own or another office then no client files or other client information should be visible.

4.3.4 Clients and visitors should never be left alone in areas where they could have access to confidential information.

Computers and IT

4.4.1 Computers must be password protected and those passwords must be changed on a regular basis (at least every [*x*] months). Passwords should not be written down or given to others.

4.4.2 Computers and other devices should be locked when not in use to minimise the risk of accidental data loss or disclosure.

4.4.3 The use of memory sticks and other removable media is prohibited. No confidential information is to be copied onto floppy disk, removable hard drive, CD or DVD or memory stick/thumb drive without the express permission of the [board OR COLP OR risk and compliance department OR IT manager] and even then it must be encrypted.

4.4.4 Data copied to any of these devices should be deleted as soon as possible and stored on our computer network in order for it to be backed up.

Backup of data

4.5.1 All electronic data must be securely backed up at the end of each working day.

4.5.2 Backup media must be encrypted.

4.5.3 Backup media that is retained on site prior to being sent for storage at a remote location must be stored securely in a locked safe and at a sufficient distance away from the original data to ensure both the original and backup copies are not compromised.

4.5.4 A recording mechanism is in place and maintained by [*insert name*] to record all backup information including any failures or other issues.

Communication and transfer

4.6.1 Confidential information must not be removed from our offices without permission from the [board OR COLP OR risk and compliance department] except where that removal is temporary and necessary (eg for attendance at court, client meetings or at a conference with counsel).

4.6.2 In such circumstances all reasonable steps must be taken to ensure that the integrity of the information and confidentiality are maintained. This will include *not*:

(a) transporting files in see-through or other un-secured bags or cases

(b) reading files in public places (waiting rooms, cafes, trains, etc)

(c) leaving files unattended or in any place where they are at risk (eg in conference rooms, car boots, cafes, etc)

4.6.3 Postal, document exchange (DX), fax 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.

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

4.6.5 Sensitive or particularly confidential information should not be sent by fax unless you can be sure that it will not be inappropriately intercepted at the recipient fax machine.

Home working

4.7.1 No confidential or other information should be taken to your home without the permission of the [board OR COLP OR risk and compliance department] and only then if they are satisfied that you have appropriate technical and practical measures in place to maintain the continued security and confidentiality of that information.

4.7.2 No confidential information is to be stored on your home computer (PC, laptop or tablet).

4.7.3 Files and confidential information must be kept in a secure and locked environment where they cannot be accessed by family members or visitors.

Overseas transfer

4.8.1 There are restrictions on international transfers of personal data. You must not transfer personal data [internationally at all OR outside the EEA (which includes the EU, Iceland, Liechtenstein and Norway) OR other than within the EEA (which includes the EU, Iceland, Liechtenstein and Norway), Switzerland, Hungary or, in some cases, Canada] without first consulting the [board OR COLP OR risk and compliance department].

Cybercrime prevention and management

5.1 All staff are required to be aware of and comply with our Cybercrime prevention strategy and incident management plan, which incorporates our:

5.1.1 Password policy

5.1.2 Remote working and removable media policy[[3]](#footnote-3)

IT system management and development

6.1 Our IT systems are managed by suitably trained staff who are responsible for overseeing day-to-day operation and to ensure continued security and integrity.

6.2 [*The IT manager*] is responsible for ensuring we have procedures for the secure configuration of network devices. These will vary from time to time but are likely to include:

6.2.1 [ensuring all network devices have up to date fire walls]

6.2.2 [encryption of hard drives]

6.2.3 [ensuring all devices are password protected/alarmed]

6.2.4 [*insert other measure or procedure*]

6.3 [*The IT manager*] is responsible for the management of user accounts and will implement procedures to ensure:

6.3.1 [appropriate permissions are set for different types of user accounts, eg administration, standard or guest]

6.3.2 [all members of staff have the correct type of user account]

6.3.3 [users run with a minimal set of permissions whenever possible]

6.3.4 [user accounts are suspended or deleted promptly where required, eg if a member of staff leaves the firm]

6.3.5 [*insert other measure or procedure*]

**[[4]](#footnote-4)**6.4 Access controls will be maintained at appropriate levels for all systems by ongoing and proactive management. Any changes to permissions must be approved by [*the IT manager*].

6.5 New IT systems, or upgrades to existing systems, must be authorised by [*the IT manager*] and the authorisation process must take account of security requirements. The information assets associated with any proposed new or updated systems must be identified and a risk assessment undertaken.

6.6 Any new equipment must have appropriate levels of resilience and fault tolerance and must be correctly maintained.

6.7 Software and applications must be managed to ensure their smooth day-to-day running and to preserve data security and integrity. The purchase or installation of new or upgraded software must be planned and managed and any information security risks must be mitigated. Specifications for new software or upgrades of existing software must specify the required information security controls. Our Software register[[5]](#footnote-5) shows all software used by the firm and who has access to different types of software. This is reviewed by [*insert name*] on a regular basis in accordance with our Information and Communication Technology (ICT) plan.

.

Business continuity

7.1 Please see the firm’s Business continuity plan. That plan has been designed to ensure continued data security and to maintain confidentiality.

Reporting breaches

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

8.1.1 investigate the failure and take remedial steps if necessary

8.1.2 maintain a register of compliance failures

8.1.3 notify the SRA of any compliance failures that are material either in their own right or as part of a pattern of failures

8.2 Please refer to our Compliance failure policy for our reporting procedure.

Training

9.1 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.

9.2 Training is provided [online AND / OR through seminars AND / OR via another training medium].

9.3 Completion of training is compulsory.

9.4 The [board OR COLP OR risk and compliance department] 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 the [board OR COLP OR risk and compliance department].

Monitoring

10.1 Everyone must observe this policy. The [board OR COLP OR risk and compliance department] has overall responsibility for this policy. They will monitor it regularly to make sure it is being adhered to.

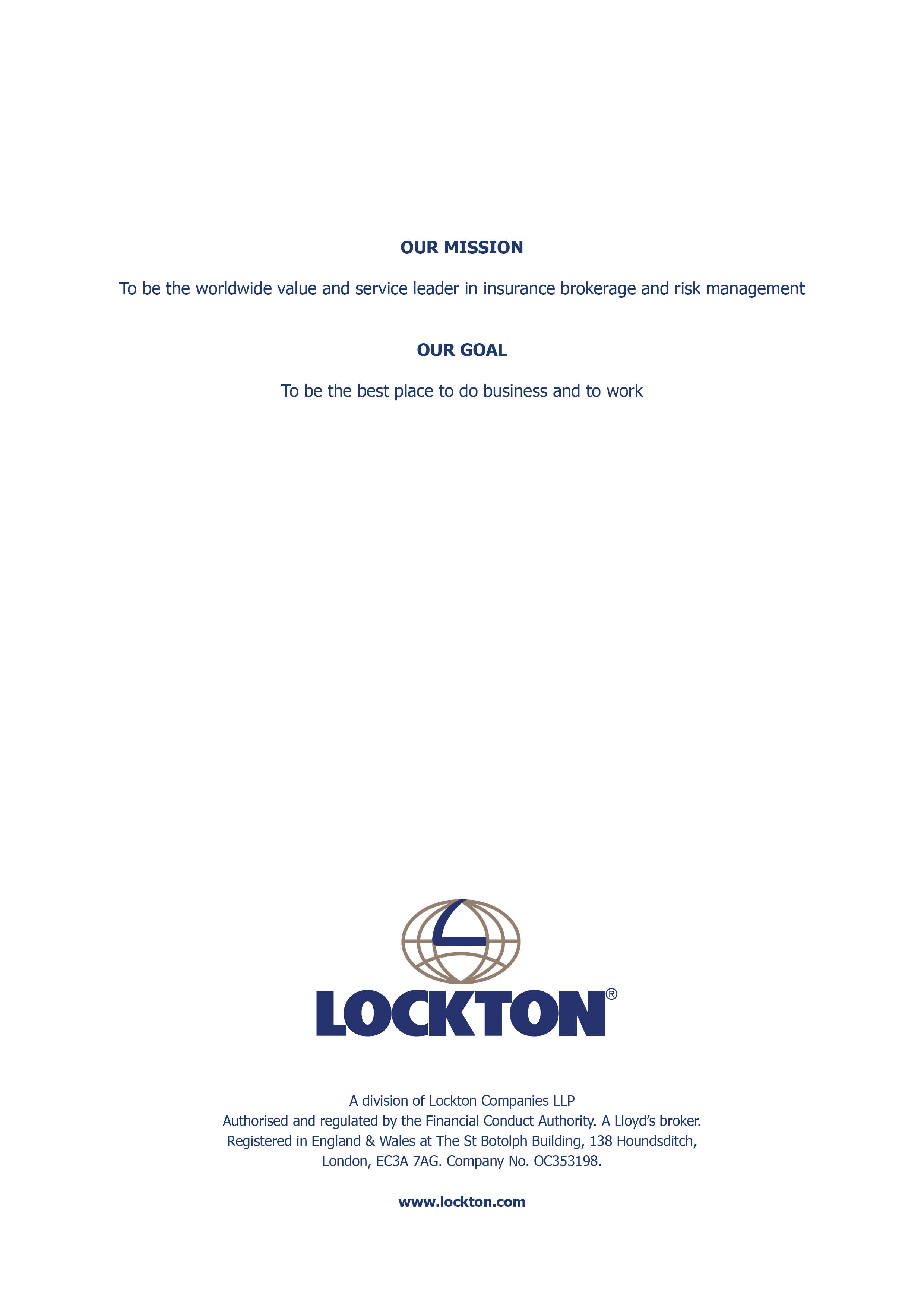
Consequences of failing to comply

11.1 We take compliance with this policy very seriously.

11.2 Failure to comply puts both you and the firm at risk.

11.3 The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures, which may result in dismissal.

11.4 If you have any questions or concerns about anything in this policy, do not hesitate to contact the [board OR COLP OR risk and compliance department].



1. *Information asset audit*

   *See separate template: Information asset audit.* [↑](#footnote-ref-1)
2. *Information asset risk assessment*

   *See separate template: Information asset risk assessment.* [↑](#footnote-ref-2)
3. [↑](#footnote-ref-3)
4. 3 Management of user accounts

   [*Lexcel v 6, para 3.1*](file:///\\Lnglondatp110\Users\OSWINJX\Word%20versions\www.lawsociety.org.uk\accreditation\lexcel\)

   *Your Information management and security policy must include procedures to manage user accounts. You should explain or give examples of what this includes.*

   4 Software register

   *See Software register and ICT plan* [↑](#footnote-ref-4)
5. *See separate template: Software register* [↑](#footnote-ref-5)