While remote working (whether at home or on the go) and removable media offer your business and clients great benefits, they can also expose you to risks that are not easy to manage. This policy explains those risks and contains suggested procedures to mitigate them.

Remote working and removable media 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®PSLPractice Compliance is an online service designed to make risk and compliance easier to manage, whatever the sizeof 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*](https://www.lexisnexis.com/uk/lexispsl/practicecompliance/home)*.*

Remote working and removable media policy

Introduction

1.1 While remote working (whether at home or on the go) and removable media offer our business and clients great benefits, they can also expose us to risks that are not easy to manage.

1.2 This policy explains those risks as well as the procedures we have in place to mitigate them.

Responsibility and application

2.1 [*Insert name*] is responsible for this policy.

2.2 This policy applies to all staff.

The risks

3.1 Remote working and removable media involve the transit and storage of confidential and sensitive data outside the secure environment of the office, usually across the internet, and sometimes in public places. This exposes us to significant risks.

3.2 Loss or theft of data

3.2.1 Mobile devices are highly susceptible to being lost or stolen and they may not have the same level of physical security as devices we keep at the office.

3.3 Public place vulnerability

3.3.1 Working remotely sometimes means working in a public place (such as a café or on a train). This presents the risk that you are overlooked, ie observed by someone else, and the security of the material you are viewing (which could potentially include confidential client information) being compromised.

3.4 Malware

3.4.1 Using removable media increases the risk of malware being introduced to our IT systems.

3.5 Reputational damage and financial instability

3.5.1 Our business is built on our reputation. Failing to keep client information secure is obviously a big threat to that.

3.5.2 Damage to our reputation can lead to financial instability (ie because our clients lose faith in us and go elsewhere for their legal needs), and direct financial loss if we are subject to fines.

Our procedures

Remote working

4.1.1 Without exception, you must be capable of operating remotely in a secure way. As a minimum, this will include:

(a) managing your user login and password details properly (see further our Password policy)

(b) being aware of your environmental surroundings and taking steps to reduce the risk of being overlooked (see Public place vulnerability, above, clause[3.3](#ukContentItemcebd061b-df6c-45de-a700-7a))

(c) using an appropriate VPN (rather than the Internet) where possible to transfer data

(d) locking your device when you are not using it

4.1.2 Only minimal data may be taken outside the office environment.

Removable media

4.2.1 Under normal circumstances information should be stored centrally on our systems and exchanged using appropriately protected and approved information exchange connections.

4.2.2 Only use removable media to store or transfer data when it is absolutely unavoidable, ie where there is no alternative.

4.2.3 Where it is necessary to use removable media, you must:

(a) obtain approval first from [*insert name*] who will scan the specific media for malware

(b) only use [*insert details of the media type(s) you will approve*] which have been formally issued by the firm

(c) not use it to store or transfer [*insert details of the types of information you do not wish to be stored or transferred using removable media*]

(d) ensure any data stored on the device is encrypted—[*insert name*] can help you

4.2.4 You should note that you are responsible for the secure use of removable media you use under this policy, including it’s safe return to the firm for destruction or re-use.

Home working

5.1 Please refer to our Information management and security policy.

Training

6.1 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.

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

6.3 Completion of training is compulsory.

6.4 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

7.1 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.

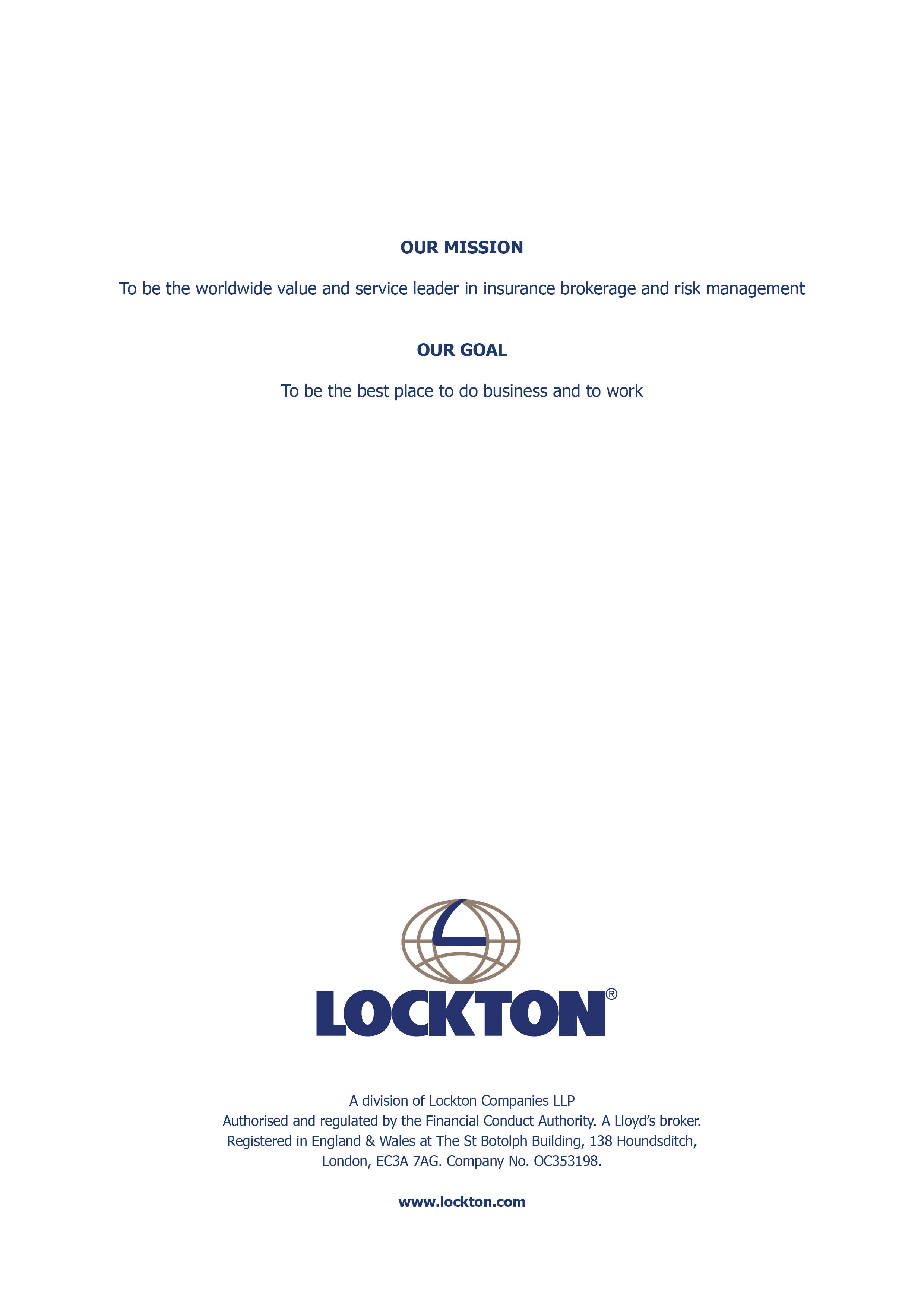
Consequences of failing to comply

8.1 We take compliance with this policy very seriously.

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

8.3 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.

8.4 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]](#footnote-1)



1. Remote working and removable media policy

   While remote working (whether at home or on the go) and removable media offer your business and clients great benefits, they can also expose you to risks that are not easy to manage. This policy explains those risks and contains suggested procedures to mitigate them.

   Information management and security policy [↑](#footnote-ref-1)