



Information security

Information security practice note - 11 September 2008

Contents

1. Introduction

1.1 Who should read this practice note?

1.2 What is the issue?

1.3 Professional conduct

1.4 Legal and other requirements

1.5 Status of this practice note

1.6 Terminology in this practice note

1.7 More information

2. Rules of professional conduct

2.1 Rule 4 - duty of confidentiality

2.2 Rule 1 - core duties

2.3 Rule 5 - supervision and management responsibilities

3. Statutory provisions

3.1 The Data Protection Act 1998 (DPA)

3.2 Regulation of Investigatory Powers Act 2000

3.3 The Computer Misuse Act 1990 (CMA)

4. Good practice for information security

4.1 Written policy

4.2 Responsibility

4.3 Reliable people

4.4 General awareness

4.5 Effective systems

5. Risk assessment

1. Introduction

1.1 Who should read this practice note?

Sole practitioners and all solicitors responsible for developing information security policies in practices
in-house solicitors, partners and others, including non-qualified staff, with an interest in information security

1.2 What is the issue?

Solicitors are increasingly vulnerable to the risk of the loss, damage or destruction of important data through theft, malicious intent or accident. This risk is growing as computers and the internet are increasingly used to process and transmit confidential client and business information.

1.3 Professional conduct

The following sections of the Solicitors' Code of Conduct 2007 (code of conduct) are relevant to information security:

Rule 1: core duties

Rule 4: duty of confidentiality

Rule 5: supervision and management responsibilities

1.4 Legal and other requirements

The following legislation is relevant to information security:

Data Protection Act 1998

Regulation of Investigatory Powers Act 2000

Computer Misuse Act 1990

1.5 Status of this practice note

Practice notes are issued by the Law Society for the use and benefit of its members. They represent the Law Society's view of good practice in a particular area. They are not intended to be the only standard of good practice that solicitors can follow. You are not required to follow them, but doing so will make it easier to account to oversight bodies for your actions .

Practice notes are not legal advice, nor do they necessarily provide a defence to complaints of misconduct or of inadequate professional service. While care has been taken to ensure that they are accurate, up to date and useful, the Law Society will not accept any legal liability in relation to them.

For queries or comments on this practice note contact the Law Society's Practice Advice Service.

1.6 Terminology in this practice note

You - solicitors' practices

Must - a specific requirement in the Solicitors' Code of Conduct or legislation. You

must comply, unless there are specific exemptions or defences provided for in the code of conduct or relevant legislation.

Should - good practice for most situations. If you deviate from this, you must be able to justify why this is appropriate, either for your firm, or in the particular retainer.

May - a non-exhaustive list of options for meeting your obligations. Which option you choose is determined by the risk profile of the individual firm, client or retainer. You must be able to justify why this was an appropriate option to oversight bodies.

1.7 More information

[Information Commissioner's website](#)

[Information security advice](#): Department for Business, Enterprise & Regulatory Reform

[Protective security advice](#): Centre for Protection of National Infrastructure

[Warning Advice and Reporting Points \(WARPs\)](#)

2 Rules of professional conduct

2.1 Rule 4 - duty of confidentiality

Rule 4 of the code of conduct sets out a general requirement of confidentiality:

'You and your firm must keep the affairs of clients and former clients confidential except where disclosure is required or permitted by law or by your client (or former client).'

You must not put a client's confidentiality at risk by acting for another client.

The rule also sets out "proper arrangements" to protect client confidentiality when acting for two or more clients whose interests are "adverse" and where "material" confidential information is held. However, these arrangements are designed with large firms and corporate clients in mind. We expect that most firms would rarely, if ever, be in a position to set up such arrangements. The guidance to rule 4 explains the situations and requirements for information barriers.

You should consider rule 4 in the wider context of the code of conduct as a whole. Two rules in particular set that context:

Rule 1: [core duties](#)

Rule 5: [supervision and management responsibilities](#)

2.2 Rule 1 - core duties

Rule 1 (core duties) requires solicitors to act with integrity, in the best interests of each client and to provide a good standard of service. It also requires a solicitor not to behave in a way that is likely to diminish the trust the public places in the solicitor or the profession. All these core duties could potentially be breached by a firm which did not operate effective information security arrangements.

2.3 Rule 5 - supervision and management responsibilities

This rule requires a principal in a firm to make arrangements for the effective management of the firm as a whole. These arrangements are detailed in the rule and explained further in the guidance to the rule. They include exercising appropriate supervision over all staff. This will include:

- setting up appropriate information security arrangements and ensuring they are implemented
- training staff in your practice to a level of competence appropriate to their work and level of responsibility
- managing risk
- ensure documents and assets entrusted to the firm are kept safe
- ensuring the practice can continue with minimum interruption to clients' business in the event of absences and emergencies

3. Statutory provisions

3.1 The Data Protection Act 1998 (DPA)

The DPA contains 8 data protection principles. The seventh principle in Schedule 1 of the DPA requires data controllers to take appropriate technical and organisational measures against both:

- unauthorised or unlawful processing of personal data, and
- accidental loss or destruction of, or damage to, personal data

To determine the appropriateness of security measures, you should consider all of the following:

- implementation costs
- technological developments
- the nature of the data - sensitive personal data will merit particular attention
- the harm that might result from unauthorised or unlawful processing or from accidental loss destruction and damage to the data

You should adopt a risk-based approach to compliance, giving appropriate weight to each of these factors. This is discussed in more depth in section 5 of this practice note.

You must also take reasonable steps to ensure the reliability of any employees who have access to the personal data. Special rules apply to contractors or others who process personal data on your behalf. See DPA Schedule 1 for guidance.

3.2 Regulation of Investigatory Powers Act 2000

If you monitor or store the electronic communications of fee-earners and other staff for business / security reasons you must comply with the relevant provisions of:

- the Regulatory and Investigatory Powers Act 2000

You should also consult Part 3 of the Information Commissioner's consolidated Employment Practices Data Protection Code. The code gives guidance for businesses on monitoring or recording e-mails in the workplace.

3.3 The Computer Misuse Act 1990 (CMA)

The Computer Misuse Act 1990 creates three computer misuse offences:

- s1: Unauthorised access to computer material
- s2: Unauthorised access with intent to commit or facilitate the commission of further offences
- s3: Unauthorised modification of computer material

A programme of information security awareness can help you to highlight these provisions within your firm.

4. Good practice for information security

The following good practice recommendations offer a foundation relevant to all practice sizes and types in developing their own, risk-based policies and procedures for information security.

4.1 Written policy

You should set out your information security practices in a written policy. The policy should reflect solicitors' professional and legal obligations. You should supplement this with implementation procedures. You should monitor these and review them at least annually.

4.2 Responsibility

You should appoint a senior member of staff to own the policy and procedures and ensure implementation.

4.3 Reliable people

You should implement and maintain effective systems to ensure the continuing reliability of all persons, including non-employees, with access to information held by the firm.

4.4 General awareness

You should ensure that all staff and contractors are aware of their duties and responsibilities under the firm's information security policy. This includes understanding how different types of information may need to be managed.

4.5 Effective systems

You should identify and invest in suitable organisational and technical systems to manage and protect the confidentiality, integrity and availability of the various types of

information you hold.

5. Risk assessment

In addition to the good practice above, you may carry out a risk-based assessment of your information security requirements to develop detailed policies and procedures that will satisfy the overall objectives of their information security policy.

A risk-based approach to information security involves identifying:

- the firm's information assets
- threats to those assets, and their likelihood and impact
- ways to reduce, avoid or transfer risk

A comprehensive risk-based assessment can be a complex task, so you may need expert advice.

Where resources do not permit a comprehensive risk-based information security assessment firms may nevertheless benefit from carrying out a basic, high-level exercise. This may help to identify any areas in which their information security is particularly weak or non-existent.

Copyright 2010 Law Society All Rights Reserved
