



The Law Society

Information security guidelines for solicitors 2006

Draft version 0.7

Business development and best practice

Important note

The Law Society Information Security Guidelines are intended to assist solicitors achieve good practice in relation to information security. At points they refer to duties which exist in professional conduct.

However, the Guidelines do not create, or extend or define the scope of, any duties of professional conduct. To determine the conduct requirements in relation to any issue described in the Guidelines, reference should be made to the relevant rules and principles of professional conduct (see www.guide.lawsociety.org.uk) and not to these Guidelines.

Contents

Introduction	5
Purpose and structure	5
Structure of the guidelines	6
Rules of professional conduct	6
Rules of professional conduct	7
Security of Records	8
Statutory provisions	9
The Data Protection Act 1998 (DPA)	9
The Regulation of Investigatory Powers Act 2000 (RIPA)	10
The Computer Misuse Act 1990 (CMA)	11
Good practice	12
Risk assessment	13
A risk-based approach	13
Identifying information assets	13
Threats, likelihood and impact	13
Risk reduction, avoidance and transfer.....	13
Conclusion	15
Annex A - Good practice recommendations	16
Written information security policy	16
Content of the policy	16
Specific policies and procedures	16
Design considerations	17
Meeting professional and legal obligations	17
Using model policies	17
Responsible person	17
The role of the responsible Partner.....	17
Supporting the responsible Partner	18
Legal and professional requirements.....	18
Further information	19
Reliable people	19
Ensuring the reliability of staff and contractors	19

Best practice	20
Legal and professional obligations.....	20
General awareness.....	20
Information security training for staff	20
Classification of information.....	21
Best practice	21
Contractors	21
Effective systems	21
Investing in information security.....	22
Technical systems	22
Annex B - Example information security policy	22
Information security policy.....	22
1. Introduction	23
2. Policy guidelines	23
2.1 Management of information security	23
2.2 Legal and regulatory compliance	24
2.3 IT systems and infrastructure.....	25
3. Other guidelines.....	25
Annex C - Data protection basics	27
Preface	27
Introductory matters	27
The Data Protection Act.....	27
Does it apply to me?	27
Complying with the DPA	27
Appointing someone to be responsible for compliance.....	28
Notifying the Information Commissioner	28
How to notify	29
'Auditing' your use of personal data.....	29
Create a 'model' of how you use data.....	29
Check compliance.....	30
First data protection principle.....	30
Second data protection principle.....	31

Third data protection principle.....	32
Fourth data protection principle	32
Fifth data protection principle.....	32
Sixth data protection principle.....	32
Seventh data protection principle.....	33
Eighth data protection principle.....	33
A written data protection policy	33
Annex C.0 - Data protection compliance process	34
Annex C.1 – Conditions relevant for purposes of first principle: processing of any personal data	35
Annex C.2 – Conditions relevant for purposes of the first principle: processing of sensitive personal data.....	36
Annex D - Practical tips on keeping confidential records securely	38
Definition of confidential material.....	38
Safeguarding the security of confidential information	39

Introduction

- 1.1 Information is a valuable asset to any firm, the loss or compromise of which can seriously affect reputation; protecting it is a management task not simply a technical IT issue. Adherence to recognised good practice, a written information security policy and periodic risk assessments should be the basis for detailed security countermeasures and procedures.
- 1.2 Solicitors have always taken measures to protect the confidentiality, integrity and availability of the information they hold. Most appreciate the time-honoured threats posed by dishonest or careless individuals; they also appreciate the additional security challenges presented by new technology and, in particular, the Internet. According to research undertaken by the Law Society the majority of law firms now have a written information security policy along with a designated individual responsible for IT security. Those that do not may be taking an unstructured approach to information security.
- 1.3 The growing complexity of information management within law firms, occasioned in part by IT developments, means that a systematic approach to information security is essential. The need to secure global electronic communications and new domestic IT-supported business processes including electronic conveyancing, electronic court filing and electronic links between the Legal Services Commission (LSC) and its suppliers, will mean that information security will continue to be an important issue for firms of all types and sizes for the foreseeable future.

Purpose and structure

- 2.1 The purpose of these guidelines is to assist principals, or others in solicitors' firms, responsible for drawing up or approving a firm's information security policy and ensuring that it is implemented. They should be regarded as complementing the Law Society's E-Mail Guidelines which similarly provide assistance in respect of e-mail policies.
- 2.2 It is important that information security is high on firms' management agenda and that this is reflected in a written information security policy which is enforced across the workplace. Such a policy will help to ensure the proper management and supervision of the practice including compliance with rules of professional conduct and statutory requirements.
- 2.3 Guidance on developing an overarching information security policy is offered in Section 5 below.
- 2.4 Firms will also need to develop detailed policies, practices and procedures to implement their information security policy. Guidance on a risk-based approach to developing such policies can be found in Section 6.

Structure of the guidelines

- 2.5 In line with this approach the guidelines have four main components which, taken together, are intended to offer firms a comprehensive and structured approach to information security.

PROFESSIONAL RULES (Section 3)	STATUTORY RULES (Section 4 & Annex C)
GOOD PRACTICE (Section 5 & Annexes A, B)	RISK ASSESSMENT (Section 6 & Annex D)

Rules of professional conduct

[NOTE: THE RULES IN THE NEW CODE OF CONDUCT ARE NOT YET IN FORCE]

- 3.1 There are professional conduct requirements which relate not just to the conduct of individuals within firms, but to firms' information security arrangements. These are set out on the Law Society's website www.lawsociety.org.uk.
- 3.2 The Law Society's Code of Conduct rule 4 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)"
- 3.3 The rule sets out a duty not to 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.
- 3.4 The requirements of rule 4 need to be set within the wider context of the Law Society's Code of Conduct as a whole. Two rules in particular set that context. Rule 1 (core duties) sets out duties of (among others) integrity, best interests of clients, competence, supervision and management, and the good repute of the profession. All these core duties could potentially be breached by a firm which did not operate effective information security arrangements.
- 3.5 The other rule which sets a context for information security issues is rule 5 (business management). This rule requires that:-
- "If you are a principal in a firm...you must make arrangements for the effective management of the firm as a whole..."
- 3.6 These "arrangements" are detailed in the rule and explained further in the Guidance to the rule. They include "compliance with the duties of a principal, in law and conduct, to exercise appropriate supervision over all staff". This will of course include setting up appropriate information security arrangements and ensuring that they are carried out. In this respect there is also a requirement for "the training of individuals working in the firm to maintain a level of competence appropriate to their work and level of responsibility" and a requirement for "the management of risk." Additionally there is a specific requirement that the "arrangements" address "the safekeeping of documents and assets entrusted to the firm".

Security of Records

- 3.7 Not all records need the same level of security. Material on a firm's website, for example, clearly does not need to be protected from public access; but if firms wish to avoid embarrassment and possible loss of reputation they do need to safeguard its integrity against hackers and malware.
- 3.8 Records also exist in many forms. They may be on paper, stored electronically, transmitted by post, e-mail or via the web, or committed to film or digital media. Appropriate protection is required for records in all formats to ensure business continuity and to avoid breaches of the law and statutory, regulatory or contractual obligations. The specific factors that affect the security of records are:
- Breaches of confidentiality.
 - Loss of data integrity and/or accessibility.
 - Corrupt employees
 - Poor information security controls
 - Organisational ignorance and lack of sophistication
- 3.9 Confidential records will always need a high level of security and the requirements are the same for all confidential records, irrespective of format. In other words, if a record contains confidential material, then it must be:
- Maintained securely for as long as it is classified as confidential.
 - Disposed of securely as soon as it is no longer needed.
- 3.10 Data integrity and accessibility should be protected through identification and investment in appropriate organisational and technical systems to manage and protect the confidentiality, integrity and availability of information assets as follows:
- Hard copy: security equipment (lockable cabinets); secure rooms with restricted access for storage of confidential records; regular review of access permissions; regular review of disaster plans.
 - Electronic: the department or person in charge of information technology should consider and regularly review:
 - Access permissions for databases or shared drives
 - Security of databases, networks, internet/intranet
 - Malware
 - Firewalls
 - Encryption
- 3.11 Practical tips for keeping confidential records securely can be found in Annex D. Firms should think about how these might fit into their overall security policy.

Statutory provisions

The Data Protection Act 1998 (DPA)

- 4.1 Solicitors, along with all other controllers of personal data, are subject to the provisions of the DPA. Data controllers must notify the Information Commissioner and it is an offence not to do so. The DPA is overseen by the Information Commissioner and the Commissioner's website (www.informationcommissioner.gov.uk) contains general guidance on the Act's requirements. Annex C below contains some basic guidelines for solicitors who are relatively new to the DPA; it includes discussion on the various data protection principles. The principle most relevant to information security is the seventh.
- 4.2 The seventh data protection principle requires data controllers to take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- 4.3 This principle is complemented by an obligation under the notification process to inform the Information Commissioner about security measures to protect personal data (see Annex C Section 3). The obligation is framed in relation to this principle as 'a general description of measures to be taken for the purpose of complying with the seventh data protection principle'.
- 4.4 To determine the appropriateness of security measures, the Act says that regard should be had to:
- implementation cost;
 - technological developments;
 - the nature of the data (sensitive personal data will merit particular attention) and
 - the harm that might result from unauthorised or unlawful processing or from accidental loss destruction and damage to the data.
- A risk-based approach to compliance will give appropriate weight to each of these factors. Section 6 of these guidelines discusses a risk-based approach to information security.
- 4.5 Firms must also take reasonable steps to ensure the reliability of any employees who have access to the personal data. Special rules apply to contractors and others who are not employees but who are processing personal data on your behalf. The Act refers to them as "data processors".
- 4.6 In order to comply with the seventh principle, you must only choose a data processor
- (a) providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out and
 - (b) take 'reasonable steps' to ensure compliance with those measures.

- 4.7 Additionally, where you use a data processor, you will not be regarded as complying with the seventh principle unless —
- (a) the processing is carried out under a contract —
 - (i) which is made or evidenced in writing, and
 - (ii) under which the data processor is to act only on instruction from [you], and
 - (b) the contract requires the data processor to comply with obligations equivalent to those imposed on [you] by the seventh principle.
- 4.8 It is important to note the breadth of the seventh principle and that it covers not just 'unlawful processing' (for example, by a hacker) but also such matters as 'accidental damage.' Compliance with the seventh data protection principle should clearly be part of a firm's overall information security policy — though a separate Data Protection Policy may also be appropriate.
- 4.9 Special rules apply to personal data relating to offences, disclosures made in connection with legal proceedings, and to processing for the purpose of obtaining legal advice or for establishing, exercising or defending legal rights.
- 4.10 Firms should also note that the seventh data protection principle requires data controllers to take steps to secure personal data. Most unencrypted e-mail is vulnerable to unauthorised access and alteration as it passes over the Internet. Firms should consider this issue in evaluating their DPA compliance, in carrying out their information security risk assessment and in drawing up detailed policies and procedures.
- 4.11 Data protection rules are complex and you are advised to allocate the responsibility for compliance to someone in the firm. This person should become familiar with the provisions of the DPA, ensure that the firm notifies the Information Commissioner of its processing and ensure that personal data is only processed in accordance with the data protection principles. In addition, data subjects broadly have the right to ask for copies of their personal data. This person can also ensure subject access requests are dealt with appropriately and within the statutory time limit of 40 days.

The Regulation of Investigatory Powers Act 2000 (RIPA)

- 4.12 If you monitor or store the electronic communications of fee-earners and other staff for business / security reasons you should be aware of the relevant provisions of RIPA and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. You should also consult Part 3 of the Information Commissioner's consolidated Employment Practices Data Protection Code which sets out guidance for businesses to consider when monitoring or recording e-mails in the work place.

- 4.13 Law Society guidelines on these matters can be found in Section 4 of the e-mail guidelines for solicitors (November 2005).

The Computer Misuse Act 1990 (CMA)

[REVISIT THIS SECTION WHEN THE POLICE AND JUSTICE BILL 2006 - CURRENTLY AWAITING 3RD READING - GETS ROYAL ASSENT]

- 4.14 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.
- 4.15 The Police and Justice Bill 2006 amends the CMA to increase the penalty for a section 1 CMA offence from six to twelve months on summary conviction and to make it indictable with a maximum penalty of two years.
- 4.16 The Bill also revises section 3 of the CMA away from 'unauthorised modification' to 'unauthorised acts with intent to impair the operation' of a computer. The maximum penalty for conviction on indictment is set at ten years.
- 4.17 Finally, the Bill creates a new offence of 'making, supplying or obtaining articles for use in computer misuse offences'. The maximum penalty, on indictment, is two years.
- 4.18 Promulgating the existence of these provisions could form part of a general programme of information security awareness (see Section 5 below).

Good practice

- 5.1 The following good practice recommendations are intended to offer a foundation that will be relevant to all sizes and types of firm in developing their own, risk-based, policies and procedures.
- 5.2 Firms may wish to adopt them as the basis for a written information security policy.

INFORMATION SECURITY GOOD PRACTICE RECOMMENDATIONS

Written policy Firms should set out their information security practices in a written policy; the policy should reflect solicitors' professional and legal obligations. The policy should be supplemented by specific policies and procedures for implementation which should be monitored and reviewed at least annually.

Responsible person Firms should appoint a Partner to own the policy and procedures and ensure they are implemented.

Reliable people Firms should take steps to ensure the continuing reliability of all those, including non-employees, with access to information held by the firm.

General awareness Firms should ensure that all staff (and where appropriate 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 looked after.

Effective systems Firms 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 they hold.

- 5.3 Each of these recommendations is discussed in detail in Annex A. As a whole they are intended to cover different aspects of information security and to provide a framework within which information security risk-assessments can be carried out.

Risk assessment

- 6.1 Firms should carry out a risk-based assessment of their information security requirements in order to develop detailed policies and procedures that will satisfy the overall objectives of their information security policy.

A risk-based approach

- 6.2 A risk-based approach to information security involves identifying:
- (i) the firm's information assets;
 - (ii) threats to those assets, and their likelihood and impact and
 - (iii) ways to reduce, avoid or transfer risk.

Identifying information assets

- 6.3 Firms probably already regard certain information as more sensitive or valuable than other information. For example, confidential client data, staff salaries or internal management papers. Each of these might form a category of information requiring a particular level of protection.
- 6.4 Identifying the various categories of information held by the firm is an essential prerequisite to securing it appropriately and effectively.

Threats, likelihood and impact

- 6.5 To map the range of threats to information assets it may help to distinguish the security objectives of confidentiality, integrity and availability. Each objective points to a different range of (sometimes overlapping) threats.¹
- 6.6 Threats are usually summarised by short descriptions. The simplest way to assess likelihood and impact is to categorise each as high, medium or low.

Risk reduction, avoidance and transfer

- 6.7 The effectiveness of countermeasures will depend on the nature and source of a threat, along with its likelihood and potential impact. Opportunities can then be found to reduce risk to an acceptable level, avoid it or transfer it (through insurance, indemnity or by agreement, for example).

¹ For example, third-party theft will compromise an information asset's confidentiality whilst staff error could affect its integrity; a power cut or a mains water leak may affect the same document's availability.

- 6.8 Some amount of risk is bound to remain. One of the advantages of a systematic approach to information security is that the level of residual risk the firm finds acceptable can be established.
- 6.9 A comprehensive risk-based assessment of information security can be a complex task. One way of ensuring that it is approached systematically is by using an appropriate template. Firms may wish to draw up their own templates but one example of the kind of template that may be helpful is illustrated below.

Information Security Risk Assessment Example Template					
Asset	Description of threat	Likelihood	Impact	Countermeasures	Residual risk
Hard copy client files	Theft by third party. Risk to confidentiality, integrity & availability of client data.	L	H	Secured premises Locked rooms Alarm system in offices Locked filing cabinets / safe Clear desk policy Visitor access procedures Staff training and awareness	L
Information in electronic comms between Office A & Office B	Access by third party	M	H	Implementation of encrypted tunnel (VPN)	L

- 6.10 It shows two different types of asset along with a description of one of the threats each faces (fire would be another threat to hard copy client files), the likelihood, impact, countermeasures and an assessment of residual risk. In this simple example, levels are ascribed to high (H), medium (M) or low (L) categories. In practice, firms will want to make a comprehensive list of all the threats to each asset and are likely to want to group types of assets together in their risk assessment tables. A straightforward H/M/L categorisation scheme may nevertheless be sufficient. Risk can be managed by reducing its likelihood or its impact. It is rarely possible to eliminate a threat though one way to do so - perhaps as a way of managing unacceptably high risk that cannot be otherwise reduced - is to cease a particular activity.
- 6.11 The task of analysing the different types of risk to different assets and identifying countermeasures is, potentially, time consuming and specialist. To some degree it is likely to be a team effort and firms may need to seek expert advice either in relation to carrying out the exercise or to identify appropriate countermeasures.
- 6.12 Where resources do not permit a comprehensive risk-based information security assessment firms may nevertheless benefit from carrying out a basic, high-level exercise

in which they consider categories of asset, risk and countermeasures. This will help to identify any areas in which their information security is particularly weak or non-existent.

Conclusion

- 7.1 Taking a rigorous approach to information security involves time, effort and cost; the immediate reward is simply the continuation of business as usual. In the longer term, it is to be hoped that the reputation of a firm that takes information security as seriously as the management of other aspects of its practice, will gradually grow in reputation.
- 7.2 Effective information security also relies heavily upon understanding and properly managing a firm's information assets. Good information management is the lifeblood of all knowledge-based professions and industries and can only contribute to a firm's overall efficiency and profitability.
- 7.3 Finally, in an increasingly interconnected, online, world the absence of effective information security will be a barrier to new business opportunities. Information security is one of the foundations of trust which will underpin the profession of solicitor in the 21st century.

Annex A - Good practice recommendations

Written information security policy

- 1.1 **Firms should set out their information security practices in a written policy; the policy should reflect solicitors' professional and legal obligations. The policy should be supplemented by specific policies and procedures for implementation which should be monitored and reviewed at least annually.**
- 1.2 Firms will already take steps to protect the business and client information they hold. Articulating the underlying policy will draw out any ambiguities or omissions and ensure that it can be communicated to all staff. It should also make it easier to review and, where necessary, revise specific policies and procedures.
- 1.3 The high-level information security objectives of most firms, set out in their written policy, are likely to be similar and will vary little over time. How each implements its policy (including the level of detail documented in supporting policies and procedures) will be geared to the characteristics of the firm and will need to be reviewed as these change.

Content of the policy

- 1.4 An overarching written information security policy is likely to set out:
 - How the firm plans to meet its professional and legal obligations in relation to information security;
 - Details of the Partner owning the policy along with any measures he or she imposes to ensure it will be implemented;
 - Processes for ensuring the reliability of those with access to the firm's data;
 - Outline of processes for raising awareness (of which a written policy is a key component);
 - The organisational and technical measures the firm will take to ensure compliance with information security.

Specific policies and procedures

- 1.5 Risk assessment is likely to drive the detailed policies and procedures that implement the overarching security policy.

Design considerations

- 1.6 Brief documents (or document sets) are more likely to be read and understood than longer documents.
- 1.7 To be effective, documents should be accessible. People need to know where they can find them and should be able to navigate through them easily. Publication on a firm's intranet or in a staff handbook can help.
- 1.8 It is also important that information security policies can be updated quickly and easily and that staff refer to the latest version. Intranets have an advantage over handbooks in this respect.

Meeting professional and legal obligations

- 1.9 An outline of law firms' main professional and legal obligations are contained in Sections 3 & 4 above. Reproducing these in an information security policy for all staff is likely to increase the size of the document and may not add much to understanding.
- 1.10 One way of approaching this is, therefore, to explain the obligation in high-level and general terms and to identify by whom and how it will be met.

Using model policies

- 1.11 Model policies can act as a useful starting point for thinking about the firms' own requirements. Reviewing a range of policies from different firms (and possibly different business sectors) is likely to be a productive exercise.
- 1.12 A generic policy is appended in Annex B of these Guidelines. It is essential that it is reviewed and amended to meet the particular circumstances and practice areas of the firm.

Responsible person

- 2.1 **Firms should appoint a Partner to own the policy and ensure it is implemented.**
- 2.2 Information security is primarily a management issue not a technical one. As with other management matters of importance, ownership at senior management level is needed.
- 2.3 It is essential that the Partner assuming responsibility for information security has the full support of the firm's management team and obtains any necessary training and support.

The role of the responsible Partner

- 2.4 In some firms the Partner with overall responsibility for the information security policy may also be responsible for drawing it up. This is more likely to be the case in the smaller firm. In larger firms, the Partner is more likely to sponsor and review an information security policy and risk-based assessment drawn up by internal and/or external advisers.
- 2.5 Information security in the firm will depend critically on the skills which the responsible Partner has or on which he can draw. A strategy for acquiring and maintaining appropriate skill levels should be drawn up. For example, detailed knowledge of in-house IT systems and their vulnerabilities may not be available in the market-place and may reside solely in the mind of a single, highly experienced, member of staff. This, in itself, is a risk.
- 2.6 Responsible Partners should familiarise themselves with the firm's broad professional and legal obligations for information security and with best practice guidelines. They should ensure that appropriately expert staff or contractors are deployed to draw up an appropriate policy, undertake a security risk analysis and ensure it is implemented. They should put procedures in place to ensure that the policy is applied, for measuring its effectiveness and for reviewing the policy and procedures as required.

Supporting the responsible Partner

- 2.7 It is desirable for a Partner to achieve an adequate level of understanding of information security issues, if necessary through appropriate training. Given the extensive nature of information security as a topic and their diverse understanding of legal and technical issues, Partners are likely to have widely differing needs. A number of commercially available courses aim to provide a good overview of the various issues for non-technical senior managers.
- 2.8 Buy-in and support from other members of the Partnership is essential in order for this role to be effective. A good understanding of the key management issues may be particularly important where the Partner is acting as advocate for the work of an internal team or external experts and may face close questioning from other members of the management team. Where the internal resource is available, a responsible Partner may consider appointing an Information Security Officer to manage the day-to-day duties of the role.

Legal and professional requirements

- 2.9 Partners have an obligation to comply with the information security requirements of the data protection. These are set out in Schedule 1 of the Data Protection Act 1998.
- [2.10 **TO BE REVISED IN LIGHT OF NEW CODE OF CONDUCT** There is also a professional duty of confidentiality and a requirement under Rule 13 of the Practice Rules for the principals in a practice to 'ensure that their practice is supervised and managed so as to provide for:

- (a) compliance with *principal* solicitors' duties at law and in conduct to exercise proper *supervision* over their admitted and unadmitted staff;

- (b) adequate *supervision* and direction of clients' matters;
- (c) compliance with the requirements of sections 22(2A) and 23(3) of the Solicitors Act 1974, section 9(4) of the Administration of Justice Act 1985 and section 84(2)(c) of the Immigration and Asylum Act 1999 as to the direction and *supervision* of unqualified persons;
- (d) effective *management* of the practice generally.]

Further information

- 2.11 An introductory guide to solicitors' obligations under the Data Protection Act can be found in Annex C. Detailed guidance is available on the Information Commissioner's website: www.ico.gov.uk

Reliable people

- 3.1 **Firms should take steps to ensure the continuing reliability of all those, including non-employees, with access to information held by the firm.**
- 3.2 The main threats — both deliberate and accidental — to the security of information comes from internal sources. Contractors may also pose a risk.
- 3.3 Firms should give consideration to information security in hiring (and firing) staff and in their overall management of staff.

Ensuring the reliability of staff and contractors

- 3.4 There are a number of key elements to ensure the reliability of staff:
- a written information security policy of which all staff (and others with access to information held by the firm) are aware (see section 1);
 - clear leadership from senior management (see section 2: responsible person);
 - ensuring proper procedures are in place for the recruitment of staff and contractors. This would include making appropriate checks and pursuing references;
 - having clear procedures for helping existing staff who may be experiencing financial or other personal difficulties;
 - ensuring proper oversight of the management of the firm (including, where appropriate, checking files, correspondence and e-mails);

Best practice

- 3.5 Written staff recruitment and management procedures are good practice and it would be appropriate to include the measures adopted to ensure the reliability of staff and others to safeguard information held by the firm.

Legal and professional obligations

- 3.6 Under the Data Protection Act data controllers must take reasonable steps to ensure the reliability of any employees who have access to personal data. (Schedule 1, Part 2, para 10).
- 3.7 The Data Protection Act also imposes an obligation on data controllers to ensure that any processing of personal data carried out on their behalf by a data processor is carried out under a contract made or evidenced in writing.

General awareness

- 4.1 **Firms should ensure that all staff (and where appropriate 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 looked after.**
- 4.2 As well as being a threat to information security, people are also the best line of defence. As well as knowing what they are themselves allowed or not allowed to do, people can also identify unusual or suspicious activity that may reveal a security breach. It is essential that they are able to recognise a range of potential threats and feel motivated to report them.

Information security training for staff

- 4.3 The purpose of awareness and training is to ensure that everyone knows what is required from them. At a certain level this is a reasonably straightforward process but there can be more complex cases and, in particular, there may need to be special and explicit rules for certain types of information.
- 4.4 Part of any awareness training should be to raise awareness of the range of threats to information security. Some staff may be attuned to thinking about information security in terms of deliberate IT-based attacks from third parties or from automated software and forget that it also involves protection of information from accidental loss or destruction. They may not be aware of the need to think about systems security alongside physical security and how daily 'housekeeping' tasks like saving and backing up data, keeping a clear desk and locking up papers at night not only helps to prevent information theft but also helps to prevent accidental loss or destruction.

Classification of information

- 4.5 Not all information needs to be protected to the same degree. Staff should be aware of any special measures that may be required to protect certain types of information. A review of the different types of information held by the firm and the information security implications should be undertaken (see Section 6: Risk assessment). It is important that staff are aware not only of how different types of information should be handled in accordance with the information security policy but also the rationale for this.

Best practice

- 4.6 Based on an analysis of the threats likely to be faced by the firm, staff should be given a clear idea of the information security situations they may be expected to deal with and the action they should take.
- 4.7 This might include a checklist of common attacks, how lack of awareness on the part of end users can lead to their being exploited by third-parties using social engineering techniques like impersonation (provision of passwords to 'administrators') and the dangers of launching programs received across the Internet.

Contractors

- 4.8 It is particularly important that contractors who are also data processors under the DPA are aware of their responsibilities. In order to comply with a contractual requirement (necessary under the Act) that such data processors comply with security obligations equivalent to those imposed on a data controller under the seventh data protection principle, it is important that contractors are made aware of what those obligations mean in practice.

Effective systems

- 5.1 **Firms 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 they hold.**
- 5.2 The rationale for this good practice recommendation is twofold. Firstly, it will help with legal compliance. The DPA requires data controllers to take 'appropriate technical and organisational measures' to protect personal data (See section 4 and Annex C). Secondly, it captures the high-level policy intent behind undertaking an information security risk-assessment. A risk-based approach helps to ensure cost-effective information security.
- 5.3 The first four good practice recommendations discussed above are the starting point for implementing this final recommendation; risk assessment to develop detailed policies and procedures (Section 6) completes the picture.

Investing in information security

- 5.4 Firms should identify a budget for expenditure on information security. In doing so they may first wish to carry out a risk assessment. According to research carried out by the DTI² the average expenditure on information security for those firms that did not carry out a risk assessment was 4% of their overall IT budget. For those firms that did carry out a risk assessment it was 7%. The DTI conclude that it was likely that 'those that have not assessed the risks are under-investing in their security.'

Technical systems

- 5.5 The main thrust of these guidelines has been the management framework within which an information security policy should be developed and implemented. Specific technical countermeasures for IT security have not been discussed. However, one of the outcomes of any risk assessment is likely to be a range of technical countermeasures.
- 5.6 The specific measures that firms need to take will depend entirely on their individual systems. If necessary, firms should seek specialist technical advice.

Annex B - Example information security policy

Important notes:

- ***This is a generic policy for information security. It should not be used before being reviewed and amended to cover the specific circumstances of your firm.***
- ***The policy should refer to other policies which firms should have in place (e.g. data protection, e-mail).***
- ***The policy does not cover disciplinary procedures which might arise as a result of breach of the policy, which should be added to this policy or dealt with separately.***
- ***This policy was last reviewed in 2006 You should regularly review your information security policy — and, in particular, your detailed policies and procedures to implement it — to take account of legislative change, changes in business processes and the outcome of risk assessment exercises.***

[Name of firm]

Information security policy

² Information security breaches survey 2006

1. Introduction

This document is the Information Security Policy for [name of firm]. It is a statement of the firm's policy for the protection of its information.

The information we hold is valuable. We need to protect it in the interests of our clients and the firm and in order to meet our legal and professional obligations.

The protection of information is the responsibility of everyone. Everyone who has access to information held by the firm should therefore read this policy and implement the measures it describes.

Information security protects information from a wide range of threats in order to ensure business continuity, minimise business damage and maximise return on investments and business opportunities. It comprises:

- (a) Confidentiality: ensuring that information is accessible only to those authorised to have access;
- (b) Integrity: safeguarding the accuracy and completeness of information and of processing methods;
- (c) Availability: ensuring that authorised users have access to information and associated assets when required.

This document defines the policy to be adopted for the protection of information throughout the firm.

2. Policy guidelines

[Name of partner in firm] on behalf of the Partners will take lead ownership of this policy and associated procedures and will champion its implementation in the firm.

2.1 Management of information security

[The Information Security Officer (ISO) or named person] is responsible for ensuring that the information security policy is implemented. [The Data Protection Officer (DPO) or named person] is responsible to [name of partner in firm] for ensuring the policy is implemented in compliance with the Data Protection Act. The Partners have ultimate responsibility for information security which they will exercise through [name of partner in firm].

Everyone with access to information is responsible for the implementation of this policy, including permanent and temporary employees, hired personnel, consultants and other contractors and third party service providers. Failure to adhere to this policy may lead to disciplinary or other appropriate action being taken.

The firm will take appropriate steps to ensure the continuing reliability of all those, including non-employees, with access to information held by the firm.

The ISO should be contacted for advice on information security. Information security training and advice is available to all employees. The DPO should be contacted for advice on data protection issues. Security incidents (such as a suspected malware infection of an IT system or a potential loss of data confidentiality, integrity or availability) should be reported to the ISO as it is important that such incidents are recorded and tracked.

2.2 Legal and regulatory compliance

There are a number of legal and regulatory requirements regarding the access, distribution and storage of information. There are also rules regarding software licensing and monitoring of usage.

The firm will seek to comply fully with the legal requirements and implications of the following legislation (and any other relevant legislation):

- The Data Protection Act 1998.
- The Regulation of Investigatory Powers Act 2000
- The Computer Misuse Act 1990.
- The Human Rights Act 1998
- Freedom of Information Act 2000
- Copyright, Designs and Patent Act 1988
- Police and Criminal Evidence Act 1984
- Health and Safety (Display Screen Equipment) Regulations 1992
- Protection of Children Act 1999

Data Protection

[Name of responsible person] will act as the firm's DPO and will ensure compliance with the requirements of the Data Protection Act and associated legislation.

This will include drawing up and maintaining the firm's data protection policy and notification. See [\[link to data protection policy\]](#).

Records Management

[Name of responsible person] will act as the firm's Records Officer and will ensure compliance with the firm's records management policy including, in collaboration with the ISO and the DPO, ensuring the security of confidential records.

This will include drawing up and maintaining the firm's records management policy.

Regulation of Investigatory Powers Act

[If applicable] The firm considers that in order to ensure compliance with policy it is necessary to monitor its communication systems. The general policy for monitoring is described below. More detailed information regarding monitoring and the firm's policy on acceptable use is described in the Detailed Guidance section.

- Compliance with this policy will be achieved by: monitoring the use of the firm's communication facilities including e-mail and Internet access; responding to

concerns regarding alleged or actual violations of this policy; and, where necessary, taking appropriate action.

- the firm reserves the right to monitor the electronic communication system and to enforce policies relating to the use of electronic information and communication systems.
- the firm also reserves the right to access information via its electronic systems when a partner or employee is not available.

2.3 IT systems and infrastructure

The firm will identify and invest in suitable organisational and technical systems to manage and protect the confidentiality, integrity and availability of the various types of information it holds.

The firm's IT systems, infrastructure and support staff will, wherever possible, maximise availability, ensure backups are taken and draw up individual disaster recovery plans for key systems.

The following cover the firm's policy guidelines for existing systems and for introducing new systems and infrastructure:

- appropriate measures will be taken to protect the firm's information and systems from damage or loss due to malicious software;
- appropriate measures will be taken to protect the confidentiality of information held by the firm;
- the availability of information will be maintained, i.e. by ensuring that information and information systems can be accessed by authorised users when required;
- information will be backed-up and the back-ups tested and business continuity plans will be produced, maintained and tested.

3. Other guidelines

Reference should be made to the following documents for more detailed guidance on the procedures that should be followed to implement the policy stated in this document. These documents can be found [...]

[For example:

The Security Manual. The Security Manual provides detailed guidance on the implementation of information security within [name of firm] . The Security Manual should be read by all persons involved in the following: the management and implementation of information security; the administration of [name of firm]'s systems; the specification and implementation of the firm's systems.

Operating Procedures. Specific operating procedures are provided for IT Administration personnel, where appropriate, to implement the requirements of the Security Manual.

Information Security User Guidance. Guidance on information security for the users of the firm's systems is provided in this document which should be read by everyone who has access to our IT systems.

Data Protection User Guidance. Guidance on the organisation's Data Protection Policy provides information on data processing, storage, access, and guidelines for complying with data protection. It should be read by everyone with access to personal data held by the firm.

Records Management Guidance. This could, for example, incorporate the material in Annex D (Practical tips on keeping confidential records securely).]

Annex C - Data protection basics

Preface

The Data Protection Act 1998 (DPA) is complex and offers much scope for interpretation. However, the application of most of the DPA to the majority of solicitors should be relatively straightforward. This guidance is intended to cover these straightforward data protection obligations and offer a framework for more detailed compliance work.

Introductory matters

The Data Protection Act

- 1.0 The Data Protection Act 1998 (DPA) regulates the processing of information relating to individuals. Solicitors must comply with the DPA. Failure to do so may constitute a criminal offence.

Does it apply to me?

- 1.1 Almost certainly. Processing personal data is fundamental to the work of a solicitor. If you, or your staff, are holding any information about a living individual on a computer (or other electronic device) then you are processing personal data and must comply with the Act.
- 1.2 It does not matter who that individual is: client, member of staff³, business partner, contact or associate. And precisely what you are doing with someone's personal data is not an issue (in this context): 'processing' includes 'any operation or set of operations on the information or data' - even deletion counts as 'processing'.
- 1.3 So how do you comply with the Act?

Complying with the DPA

- 1.4 We recommend seven steps to compliance:
 - appoint someone to be responsible for compliance (this could be you);
 - notify the Information Commissioner;
 - 'audit' your use of personal data;
 - check compliance against the data protection principles and
 - draw up and implement a data protection policy.
 - publicise your policy (e.g. links on website and reference in letter of engagement);

³ Special rules on notification apply if you are only processing data about staff.

- train your lawyers and staff

1.5 This process is illustrated in Annex A.

Appointing someone to be responsible for compliance

- 2.0 The first step in complying with the DPA is to ensure that someone with appropriate authority takes the lead. The main duties of that person will be to:
- (i) familiarise themselves with the Act, guidance and relevant case law and keep abreast of changes;
 - (ii) notify the Information Commissioner, keep the notification up to date and renew it annually;
 - (iii) regularly 'audit' the firm's use of personal data and check compliance;
 - (ii) draw up a written data protection policy and ensure that other members of staff are aware of, understand and comply with it; and
 - (iii) take the lead to ensure that data subject access (and other legitimate DPA) requests are handled timeously.
- 2.1 Appointing a responsible person is not a requirement of the Act. It is simply good management. Larger firms are likely to appoint a specialist data protection officer (who, in turn, may report to a senior partner).

Notifying the Information Commissioner

- 3.0 One of the first (and most urgent) tasks of the responsible person is to ensure that the Information Commissioner has been notified of data processing.
- 3.1 The Information Commissioner oversees the DPA. The Act says that you cannot process personal data unless you have provided him with your 'registrable details' and a general description of the security measures you will take to protect personal data.
- 3.2 Registrable details include your name and address, a description of the personal data you are processing and the purposes for which you are processing them. The Information Commissioner enters this information on the Public Register of Data Controllers which can be accessed via his website (www.informationcommissioner.gov.uk).
- 3.3 Processing personal data without notifying the Information Commissioner is an offence.
- 3.4 Do not assume that because the Information Commissioner has not contacted you, you do not need to notify him. You have an obligation to notify. The Information Commissioner does not have to inform you, or remind you, of this. The majority of solicitors' firms have notified the Information Commissioner; those who have not risk a fine.

How to notify

- 3.5 Notification is straightforward. It involves completing a form. This can be done:
- (a) over the Internet (www.informationcommissioner.gov.uk), but note that the form will have to be printed off and signed;
 - (b) by telephone via the Notification helpline (01625 545740) where assistance will be given with completing the form which will then be sent to you or
 - (c) hardcopy. You can request a form by writing to the Information Commissioner.
- 3.6 A fee of £35 will be charged for notification. Annual renewal costs an additional £35.

'Auditing' your use of personal data

- 4.0 If you are processing personal data — and have notified the Information Commissioner — you should make sure you understand your data and your processing. Your notification to the Information Commissioner offers a starting point. In completing it you will have made a high-level sketch of your processing; it will now be helpful to fill in *some* of the detail.

Create a 'model' of how you use data

- 4.1 Try to identify the different categories of individual about whom you process personal information (clients, business partners etc) and the various sources from which you receive that information (directly from the individual themselves or indirectly through other people). Then be sure you understand where that information is kept (on a central data store, on local machines, in e-mail accounts etc) and what is done with it (who has access to it, who it is shared with etc).
- 4.2 In a small firm this need not be an elaborate exercise though, to get a complete picture, it will often be necessary to ask other members of the firm about their use of data. Doing so will act as a useful double-check against your own understanding. You should end up with a basic model of the personal data you are processing.
- 4.3 There is no need to formalise your model and constructing one is not a requirement of the Act but keeping rough notes and / or diagrams that help you to understand the way you use personal data should be a great help when you move on to consider compliance with the DPA. Above all, you will want to avoid missing entire categories of data processing from your compliance check.

Check compliance

- 5.0 Once you have a reasonably good idea of how you use personal data you can start checking whether or not your use complies with the DPA. The Act sets out eight data protection principles with which you must comply. Check your data processing against each principle.
- 5.1 The notes below should help you to get started but we recommend that you read carefully the principles and their interpretation which can be found in the DPA Schedule 1, Part I (principles) and Part II (interpretation).

First data protection principle

- 5.2 The first data protection principle states that personal data shall be processed 'fairly and lawfully' and shall not be processed unless:
- (a) at least one of the conditions in Schedule 2 is met, and
 - (b) in the case of sensitive personal data at least one of the conditions in Schedule 3 is also met.
- 5.3 Schedule 2 is set out in Annex C.1 and Schedule 3 in Annex C.2. Sensitive personal data is defined as personal data consisting of information as to —
- (a) the racial or ethnic origin of the data subject,
 - (b) his political opinions,
 - (c) his religious beliefs or other beliefs of a similar nature,
 - (d) whether he is a member of a trade union,
 - (e) his physical or mental health or condition,
 - (f) his sexual life,
 - (g) the commission or alleged commission by him of any offence, or
 - (h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.
- 5.4 To check compliance with the first data protection principle you could list all the data you process and ensure that in each case a Schedule 2 condition has been met. You could then check that, where required, at least one Schedule 3 condition has also been met.

eg:

Description of processing	Schedule 2 condition	Schedule 3 condition (where applicable)
Contract negotiations	Condition 2(b) - necessary for taking steps to enter a contract at the request of the data subject	Condition 1 : explicit consent by the data subject

- 5.5 The first data protection principle has other requirements (these are set out in the interpretation). You should consider:
- (a) *Whether or not you have misled anyone.* To assess whether personal data are processed fairly you should look at how they have been obtained and, in particular, 'whether any person from whom they are obtained is deceived or misled as to the purpose or purposes for which they are to be processed'.
 - (b) *How you have satisfied the basic information requirements.* Have you informed data subjects of your identity, the purpose or purposes for which the data are intended to be processed and anything else which you think is necessary in order to make the processing fair?
 - (c) *Have you complied with any additional, special, rules?* Special rules apply to the collection and processing of personal information by e-mail etc and, in particular, unsolicited electronic marketing communications. These are covered by the Privacy and Electronic Communications (EC Directive) Regulations 2003. You can consult the *Law Society's E-Mail Guidelines for Solicitors 2005* for further information.

Second data protection principle

- 5.5 The second data protection principle states that personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
- 5.6 'Purpose' runs like a thread through the whole Act. It is a significant feature of the first principle. This is explicit in the requirements not to mislead as to the purpose of processing and to inform people about those purposes. It is implicit in the requirement to identify Schedule 2 and Schedule 3 conditions which can only be done by reference to the purpose of the processing (for example, has there been consent to processing for such and such a purpose; is the processing necessary for a particular purpose). The centrality of 'purpose' is reinforced in the other data protection principles and most clearly in the second principle.
- 5.7 In complying with the second data protection principle your first step should be to check whether or not a purpose for obtaining the data has been specified (generally, the person concerned should have been informed of this purpose in order to comply with the first principle) and ensure it is lawful. If processing clearly falls within this purpose then it is unnecessary to proceed to ask whether the processing is 'compatible' with the original processing.

Third data protection principle

- 5.8 The third data protection principle states that personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- 5.9 It is worth noting that as well as requiring personal data to be relevant, the principle points in two directions — enough information must be held for a particular purpose (adequacy), but not too much.

Fourth data protection principle

- 5.10 The fourth data protection principle states that personal data shall be accurate and, where necessary, kept up to date. The Act defines inaccurate data as 'incorrect or misleading as to any matter of fact.'
- 5.11 Inaccurate data that accurately record the information you have been given do not contravene the fourth principle if you have taken reasonable steps to ensure their accuracy (what is reasonable depends on the purpose of the processing) and if, where the person it concerns has notified you that it is inaccurate, you have included this in the data.

Fifth data protection principle

- 5.12 The fifth data protection principle states that personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- 5.13 Setting up data retention and review schedules for categories of personal data will help you comply with this principle. The idea is that, after a set period of time, the data are reviewed and if they no longer need to be retained, are destroyed.

Sixth data protection principle

- 5.14 The sixth data protection principle requires that personal data be processed in accordance with the rights of data subjects under the Act.
- 5.15 The DPA gives data subjects a number of rights. Perhaps the most important is the right to have access to their personal data (discussed further in section 7 below) but there are also rights to prevent processing for purposes of direct marketing, rights in relation to automated decision-taking and a right to prevent processing likely to cause damage or distress.

Seventh data protection principle

- 5.16 The seventh data protection principle requires data controllers to take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- 5.17 It is discussed in the main body of the information security guidelines (see Section 4).

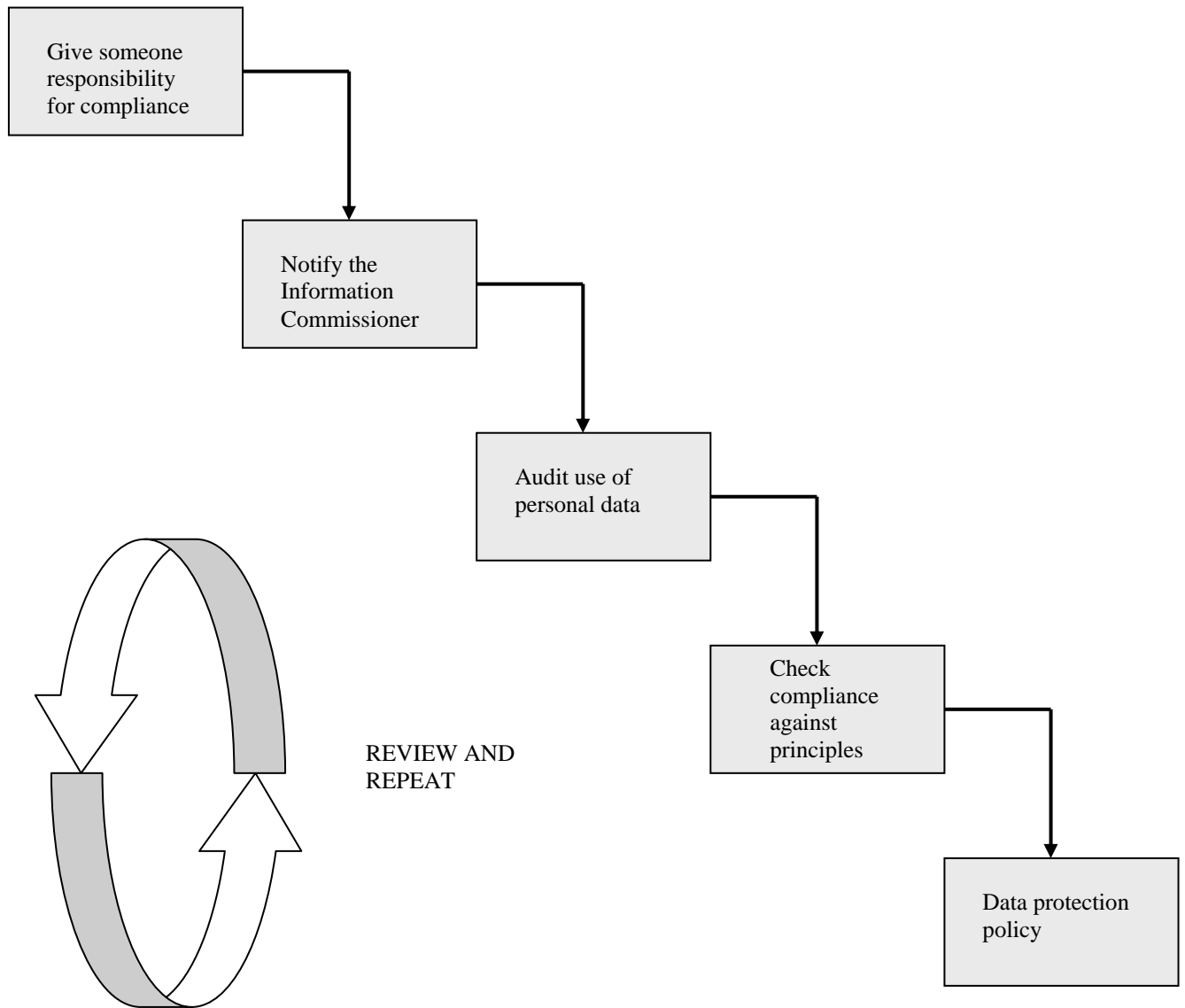
Eighth data protection principle

- 5.23 The eighth data protection principle states that personal data shall not be transferred to a country or territory outside the European Economic Area (EEA) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.
- 5.24 The EEA encompasses the European Union (EU) along with Iceland, Liechtenstein and Norway. EU findings of adequacy have been made in respect of Switzerland, Hungary and (partially) Canada. 'Safe Harbor' arrangements with individual companies in the United States (US) have been in operation since 2000. The scheme is enforced by the US Federal Trade Commission.
- 5.25 If you are considering transferring personal data overseas you should consult more detailed guidance (see bibliography).

A written data protection policy

- 6.0 A written data protection policy is not a requirement of the DPA. Drawing one up will, however, provide a systematic way to help ensure compliance; additionally, if you have staff, it will help to inform them about their own duties under the Act.
- 6.1 A typical data protection policy might cover the following:
- The general principles of the Act and the obligation of all members of the firm to help ensure full compliance;
 - Who is responsible for taking the lead on compliance and when the circumstances in which they should be contacted or consulted (provide full contact details)
 - How to deal with internal (staff) and external (other data subject) access requests (usually it will be only be necessary for staff to recognise an access request before passing it on to whoever is responsible for compliance)
 - Staff responsibility for personal data
 - Information security procedures (this may involve cross-referencing to an information security policy document).

Annex C.0 - Data protection compliance process



Annex C.1 – Conditions relevant for purposes of first principle: processing of any personal data

1. The data subject has given his consent to the processing.
2. The processing is necessary —
 - (a) for the performance of a contract to which the data subject is a party, or
 - (b) for the taking of steps at the request of the data subject with a view to entering into a contract.
3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.
4. The processing is necessary in order to protect the vital interests of the data subject.
5. The processing is necessary —
 - (a) for the administration of justice,
 - (b) for the exercise of any functions of either House of Parliament,
 - (c) for the exercise of any functions conferred on any person by or under any enactment,
 - (d) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or
 - (e) for the exercise of any other functions of a public nature exercised in the public interest by any person.
6. —(1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.
(2) The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

Annex C.2 – Conditions relevant for purposes of the first principle: processing of sensitive personal data

1. The data subject has given his explicit consent to the processing of the personal data.
2. - (1) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

(2) The Secretary of State may by order-
 - (a) exclude the application of sub-paragraph (1) in such cases as may be specified, or
 - (b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied
3. The processing is necessary-
 - (a) in order to protect the vital interests of the data subject or another person, in a case where-
 - (i) consent cannot be given by or on behalf of the data subject, or
 - (ii) the data controller cannot reasonably be expected to obtain the consent of the data subject, or
 - (b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.
4. The processing-
 - (a) is carried out in the course of its legitimate activities by any body or association which-
 - (i) is not established or conducted for profit, and
 - (ii) exists for political, philosophical, religious or trade-union purposes,
 - (b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,
 - (c) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and
 - (d) does not involve disclosure of the personal data to a third party without the consent of the data subject.
5. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.
6. The processing-
 - (a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
 - (b) is necessary for the purpose of obtaining legal advice, or
 - (c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.
7. - (1) The processing is necessary-
 - (a) for the administration of justice,
 - (b) for the exercise of any functions conferred on any person by or under an enactment, or

(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

(2) The Secretary of State may by order-

(a) exclude the application of sub-paragraph (1) in such cases as may be specified, or

(b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

8. (1) The processing is necessary for medical purposes and is undertaken by-
- (a) a health professional, or
 - (b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

(2) In this paragraph "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

9. - (1) The processing-

- (a) is of sensitive personal data consisting of information as to racial or ethnic origin,
- (b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and
- (c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

(2) The Secretary of State may by order specify circumstances in which processing falling within sub-paragraph (1)(a) and (b) is, or is not, to be taken for the purposes of sub-paragraph (1)(c) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.

10. The personal data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph.

Annex D - Practical tips on keeping confidential records securely

Please note these are suggestions and firms should consider them as part of their review of overall requirements.

Definition of confidential material

1. Any record which contains personal information about a living individual e.g.

- Questionnaire or other data collected under an express or implied guarantee of confidentiality.
- Correspondence or other documents which reveal the contact details (including home or personal e-mail address) or any financial details of a named living person, unless permission has been given to circulate the details.
- Correspondence or other documents which reveal personal details or pass comments on a named living person.
- Staff interview or counselling records
- Personnel records
- Records of disciplinary cases
- Student records, including academic progress and welfare
- Grant applications
- Job applications
- Interview notes
- Admissions records
- Redundancy records
- Sick pay records
- Maternity pay records
- Income tax and National Insurance returns
- Wages and salary records
- Accident books and records
- Health records
- Medical records

2. Any record which, if made public before a certain period, may breach commercial confidentiality e.g.

- Contracts
- Tenders
- Purchasing records
- Maintenance records
- Insurance records
- Unpublished accounting records
- Commercial, corporate or design information provided by an organisation or individual under an assurance that it would not be disclosed
- Sensitive industrial relations negotiation material
- Internal audit and protective security reports
- Corporate legal documents having a bearing on a law enforcement or current court action

3. Any record, the release of which may breach intellectual property rights e.g.

- Unpublished research material, drafts and manuscripts.

Safeguarding the security of confidential information

1. Electronic information

- Access to confidential records should be password protected and authorisation levels clearly documented and regularly updated.
- Workstations should be switched off or locked when not in use.
- Where information is taken outside the firm the same duty of care applies as in the workplace. Special care should be taken when using portable devices such as laptops, to ensure that confidentiality is not compromised (e.g. through overlooking by members of the public), and that back-ups and malware protection measures are regularly undertaken.
- All removable media such as tapes, microfilm or disks should be stored in a safe, secure environment in accordance with the manufacturers' specifications.
- E-mail is not a secure medium; staff should be advised on its appropriate use in relation to the transmission of confidential material through training sessions and provision of guidelines.
- Encryption should always be used where security is paramount.

2. Paper records

- Confidential records should carry an appropriate classification label (though beware attracting unwelcome attention to documents).
- File titles should be worded so that confidential information (e.g. someone's address) is not included in the title.
- A clear desk policy should be standard practice when dealing with confidential paper files unless you are confident that whatever other arrangements are made (for example, a secured area, vetted staff) ensure the requisite level of security.
- Filing cabinets containing confidential material should be locked at all times when not in use. Make sure, however, that material is accessible when needed.
- A list of persons authorised to access and/or maintain confidential records should be kept and reviewed regularly. This may, of course, include all current members of the firm.
- Faxes should only be used to transmit confidential information where the security status of the receiving machine is assured.
- Non-current confidential records which need to be kept for a specified period prior to destruction should be transferred to a secure records store, either in-house or provided by a suitably vetted commercial storage firm.

3. Destruction of confidential data:

- Confidential material in paper format should be shredded.
- Care should equally be taken with deletion of electronic records, which can be reconstructed from deleted information. Final deletion should be carried out in collaboration with the relevant IT support team or person to ensure that the deleted data can no longer be recovered.

4. Incident Response:

A firm that fails to take on a formal incident response, or simply a 'patch and proceed' approach is going to fall short of recognised best practices. An effective response to such incidents is needed, as well as the tools to address the problem.

For many the incident response process is either non-existent or simply consists of attempting to patch systems and restore them to a perceived previous state. The typical incident response is often hit and miss or ad hoc at best.

However information security can be achieved by implementing an appropriate set of controls and to maintain these, firms should establish procedures that make certain of a rapid, effective, efficient and methodical response to security incidents. These procedures should guarantee the reporting of an incident to an appropriate authority. The firm that has suffered a security breach needs to properly collect evidence in relation to a potential breach of contract, breach of regulatory requirement or in the event of civil or criminal proceedings.

This requires that the evidence be collected in a forensically sound manner, which means that they should ensure that their information systems comply with the requirements pertinent to the production of admissible evidence.

When an incident is initially detected, it may not be apparent that it will result in probable proceedings, therefore, the danger exists that necessary evidence is destroyed before the seriousness of the incident is realised.