

Chapter 3

Information sharing

Summary

- Under the Civil Contingencies Act, Category 1 and 2 responders have a duty to share information with other Category 1 and 2 responders. Information sharing is also encouraged as being good practice.
- Information sharing is a crucial element of civil protection work, underpinning all forms of co-operation. Category 1 and 2 responders should share information formally and as part of a culture of co-operation (paragraphs 3.1–3.6 and Chapter 2).
- The initial presumption is that all information should be shared, but the release of some information, and of information to some audiences, may need to be controlled. Category 1 and 2 responders need to understand what should be controlled (paragraphs 3.7–3.15).
- Category 1 responders need to know how to categorise types of information; how the different types of information can be used; how to obtain consent; and the limits on disclosure (paragraphs 3.16–3.31).
- Category 1 and 2 responders need to know about the impact of other legislation, such as the Freedom of Information and Data Protection Acts, on their information sharing (paragraphs 3.48–3.58).

What the Act and the Regulations require

Purpose and scope

3.1 Information is shared between Category 1 and 2 responders as they work together to perform their duties under the Act. Information sharing is a crucial element of civil protection work, underpinning all forms of co-operation. It may involve simple liaison between bodies keeping each other up to date on their current arrangements and future plans. Such activities may be carried out through the proposed forums, and more informally.

3.2 Information sharing may also involve direct contacts, formal or informal, between Category 1 and 2 responders seeking knowledge of hazards, risk assessments or planning arrangements (including warning procedures) and other matters, where the information is in the possession of one, and the other believes it needs the information to fulfil its civil protection duties.

3.3 The process of sharing information is crucial to other elements of the duty:

- Sound risk assessment relies on obtaining accurate information about the nature of the hazard, the probability of a hazardous event occurring, and the potential effects and impact on the community if it does. Each of these elements may involve some specialist knowledge and calculation and the information required may be privileged or sensitive and not generally in the public domain.
- Business continuity management largely involves knowledge of the vulnerabilities of one's own organisation – but it also examines linkages to and dependencies on suppliers and contractors, where information may be harder to obtain.
- Emergency planning relies essentially on knowledge of how each of your partners in response has planned to perform – what their aims and contribution will be, how they will organise and co-ordinate their efforts with those of other bodies, and how contacts will be managed before and during the event. All these details are constantly changing as plans are revised, organisations are restructured or their roles redefined, and individuals and teams are replaced.

3.4 Information sharing is necessary so that Category 1 and 2 responders are able to make the right judgements. If Category 1 and 2 responders have access to all the information they need, they can make the right decisions about how to plan and what to plan for. If they do not have access to all information, their planning will be weakened. They will be less well placed to make judgements around cost-benefit analysis – what to plan for and what not to plan for.

3.5 But the picture is complicated because each individual Category 1 or 2 responder needs to get its planning right and this has to be balanced against the needs of others. For example, sharing a piece of information which helps the planning of one Category 1 or 2 responder could harm the interests of another Category 1 or 2 responder. Also, the perspective of an individual organisation on a single piece of information can be affected by its own position, so an organisation can interpret information in a way that seems correct but is actually wrong. For example, a Category 1 or 2 responder might interpret something to be a risk, but another Category 1 or 2 responder with greater expertise might be less concerned. And in some circumstances, Category 1 or 2 responders will not be able to appreciate the bigger picture into which the information fits. For example, a seemingly innocuous piece of information might have implications for national security.

3.6 These two competing factors point towards a framework in which the initial presumption is that information should be shared, but that some information should be controlled if its release would be counterproductive or damaging in some other way.

When information should not be formally requested

3.7 In most instances, information will pass freely between Category 1 and 2 responders, as part of a more general process of dialogue and co-operation. This is the means by which the overwhelming majority of information sharing should happen and has happened. If this is not the case, it is probably evidence of a wider systemic failing in the way the Act is operating in the local area in question.

3.8 As a consequence, the Regulations¹ require Category 1 and 2 responders to consider alternative routes before pursuing a formal information request. This ensures that Category 1 and 2 responders make proper efforts to use existing and informal routes to gather information. The aim of this provision is to avoid over-bureaucratisation of the information-sharing process, and reinforce the message that the information-sharing mechanisms under the Act should be regarded as a fallback rather than as the first option.

3.9 Firstly, the Category 1 or 2 responder must be satisfied that it does not already hold the information, either by virtue of a previous request or because of informal information exchange. Category 1 and 2 responders should, as a consequence, marshal the information they hold in such a way as to ensure they can make a judgement on this point.

3.10 Secondly, the Category 1 or 2 responder must satisfy itself that the information is not reasonably accessible to the public – that is to say, is not put out generally by the Category 1 or 2 responder as part of its wider information policy. Examples of this would include material made available in annual reports or accounts, or material on websites (both those of individual Category 1 or 2 responders and general websites with generic information such as <http://www.ukresilience.info>).

3.11 Thirdly, the Category 1 or 2 responder must satisfy itself that the information cannot be obtained by other means. This includes all forms of informal dialogue and information sharing, and obliges Category 1 and 2 responders to work together in the first instance to agree information flows that meet the need of those organisations involved. These will include many of the informal information-sharing agreements that exist at the local level. Category 1 and 2 responders also have or may have pre-existing requirements on them under other legislation (including, for example, their licence conditions from a regulator, or by direction of a minister) to assess risk and to prepare planning arrangements for emergencies. This may mean that relationships and information-sharing routes are already established.

Where possible, these should be built on and complemented, rather than duplicated.

Formal procedures for requesting information

Procedure for making a request

3.12 But there are still some instances in which the supply of information will be more controlled. Under the Regulations, any Category 1 or 2 responder can request information from another Category 1 or 2 responder, so long as it is for the purpose of fulfilling responsibilities under the Act, or the performance of another function which relates to an emergency.² This should be seen very much as a fallback option, and every effort should be made to maintain relationships between Category 1 and 2 responders that allow information to be shared without recourse to formal requests. But should formal requests be necessary, there are a number of procedures that need to be followed in order to make the system work.

3.13 In any instance of information sharing, one or more Category 1 or 2 responders will request the information and one or more will receive the request. They are known respectively as “the requesting Category 1 or 2 responder” and “the receiving Category 1 or 2 responder.”³

3.14 A full explanation of the formal procedures for requesting information is set out at Annex 3A.

3.15 Templates for making and replying to information requests can be found at Annex 3B.

Sensitive information

3.16 Not all information can be shared, and Category 1 and 2 responders can claim exceptions in certain circumstances (and thus not supply information as requested). Exceptions under this Act and the Regulations relate to sensitive information only. Where the exceptions apply, a Category 1 or 2 responder must not disclose the information:

- **Exception where disclosure would prejudice sensitive information:** A Category 1 or 2 responder must refuse to comply with an information request if the information is sensitive

¹ regulation 47(3)(b)

² regulation 47

³ regulation 47

and if it has reasonable grounds to believe that complying with the request would compromise that information. If a Category 1 or 2 responder refuses to disclose information on this basis, it must give reasons for so doing, unless the information is sensitive by virtue of its impact on national security.⁴ For example, one Category 1 or 2 responder might be unwilling to pass sensitive information to another Category 1 or 2 responder because the latter was known to have problems with its employees leaking information to the media. It should be noted, however, that this exception is only rarely likely to be available, as generally there will be no robust reason to expect that information would be passed on.

- **Exception where information has been supplied by the intelligence services:** Where a Category 1 or 2 responder receives an information request in relation to information which has been supplied directly or indirectly by the intelligence services (the Security Service, Secret Intelligence Service, Government Communications Headquarters or National Criminal Intelligence Service), the responder must not comply with the request unless the relevant intelligence service consents to the disclosure of the information. The intelligence service may impose conditions on its consent.⁵

3.17 There are four different kinds of sensitive information as defined by the Regulations:⁶

- **Information prejudicial to national security** – information, the disclosure of which to the public would adversely affect national security.
- **Information prejudicial to public safety** – information, the disclosure of which to the public would adversely affect public safety.
- **Commercially sensitive information** – information which relates to the business or other affairs of a person or organisation, and disclosure of which to the public would prejudice the legitimate business interests of the person or organisation to whom the information relates.
- **Personal information** – information which is personal data within the meaning of the Data Protection Act 1998 (DPA), disclosure of which to the public would breach any of the data protection principles or section 10 of the DPA.

3.18 It will be for individual Category 1 or 2 responders to reach a decision about whether the information they hold is sensitive. But there are a number of general points that should affect the decision:

- All Category 1 and 2 responders should work on the presumption that information requested should be disclosed. Non-disclosure should only occur in exceptional cases, such as where there are national security implications.
- Where the Category 1 or 2 responder knows that the information has originated from the intelligence services and that disclosure to the public would threaten national security, then the information must not be disclosed. Where the Category 1 or 2 responder suspects that the information has originated from the intelligence services or that it may be sensitive for reasons of national security, it should consult with the originator of the information. However, material that originates from the intelligence services is not, as a matter of course, sensitive information.
- In considering national security implications, note that the test is whether disclosure to the public would threaten national security, not whether disclosure to the requesting Category 1 or 2 responder would threaten national security. A similar test applies in the other categories of sensitive information.
- In the case of information that is sensitive by virtue of its national security implications, a Minister of the Crown may issue a certificate certifying that disclosure of that information to the public would be contrary to the interests of national security. This certificate is conclusive. The Minister can issue a certificate in relation to a class of information or a specific piece of information. Note, however, that absence of a certificate does not mean that the information cannot be sensitive on national security grounds.⁷
- Where a request relates to information, part of which is sensitive and part of which is not, the exception only applies to the sensitive information. (In other words, the application of an exception does not necessarily enable a Category 1 or 2 responder to refuse an information request in its entirety.)

⁴ regulation 45(1)

⁵ regulation 49(4)

⁶ regulation 45(1)

⁷ regulation 46

Using non-sensitive information

Use within the planning process

3.19 The Act and Regulations do not impose any limits on the use of information obtained under the Act which is not sensitive. However, use of non-sensitive information may be limited by duties of confidence, by other enactment or by contract.

3.20 There are unlikely to be any restrictions on the use to which a Category 1 or 2 responder can put non-sensitive information which it creates in the course of carrying on its duties under the Act (eg an emergency plan – though an emergency plan may contain information that has been supplied by another Category 1 or 2 responder, and the use to which this information may be put may be subject to limits). It is also important to be mindful that information is sensitive within different environments, and whilst some information may be suitable for sharing among Category 1 or 2 responders it might not be suitable for the wider public.

Disclosure

3.21 Neither the Act nor the Regulations place any restriction on the disclosure of non-sensitive information that is obtained under the Act. Nor do the Act or Regulations create any restriction on disclosure of non-sensitive information that is created by a Category 1 or 2 responder in the course of carrying out its functions under the Act. However, non-sensitive information which is received from other Category 1 or 2 responders or third parties may be subject to a duty of confidence or contractual restrictions on disclosure. Category 1 or 2 responders may also be subject to other statutory restrictions on disclosure.

3.22 Just because there is no restriction on disclosure, this does not necessarily mean that the Category 1 or 2 responder will be obliged to disclose the information. But some Category 1 or 2 responders may be under a legal obligation to disclose certain information – in particular, under the Act (see, for example, the duty to arrange to publish in part the plans and risk assessments),⁸ the Freedom of

Information Act 2000 and the Environmental Information Regulations 2004.⁹

Using sensitive information

Use within the planning process

3.23 Sensitive information reasonably requested by a Category 1 responder in performance of its functions to deal with an emergency may only be used for the purpose of performing the function for which it was requested. In other words, if a Category 1 responder asks for sensitive information for the purpose of performing a particular function under its regulatory regime, that information may only be used for that purpose.¹⁰ The effect of this will be to limit the circulation of information within Category 1 responder organisations. For example, information about the robustness of mobile phone coverage in the event of an emergency, legitimately obtained by one part of an organisation for use in emergency plans, should not be shared with another part of the organisation responsible for the organisation's contractual relationship with its mobile phone provider.

3.24 If a Category 1 or 2 responder wishes to use sensitive information it has received by virtue of an information request under the Act for a different purpose, it must obtain the consent of the relevant person or organisation. The relevant person or organisation for different types of sensitive information is set out in Figure 3.1.¹¹

3.25 The use of sensitive information may be further restricted by duties of confidence, by other enactment or by contract.

3.26 Restrictions on the disclosure of sensitive information which is created by a Category 1 or 2 responder in the course of carrying out its duties under the Act are dealt with below. This is likely to limit the way in which sensitive information created by a Category 1 or 2 responder is used.

Disclosure

3.27 The Regulations prohibit any Category 1 and 2 responder from publishing or otherwise disclosing

⁸s. 2(1)(f)

⁹S.I.2004/3391

¹⁰regulation 52(1)

¹¹regulation 52(2)

Figure 3.1: Relevant persons or organisations for different types of security information

Type of sensitive information	Person or organisation whose consent is needed
Relates to national security and supplied indirectly or directly by one of the intelligence services	Minister of the Crown OR the intelligence service which supplied the information
Relates to national security but not supplied indirectly or directly by one of the intelligence services	Minister of the Crown OR (a) if the information is contained in a document which has been created by a public authority, that authority; (b) in other cases, the organisation which supplied the information
Relates to public safety and supplied indirectly or directly by one of the intelligence services	Minister of the Crown OR the intelligence service which supplied the information
Relates to public safety but not supplied indirectly or directly by one of the intelligence services	Minister of the Crown OR (a) if the information is contained in a document which has been created by a public authority, that authority; (b) in other cases, the organisation that supplied the information
Relates to the business or other affairs of a person or organisation where disclosure would harm the legitimate business interests of that person or organisation	The person or organisation to whom the information relates
Is personal data (within the meaning of the Data Protection Act 1998) where disclosure would contravene the data protection principles/ section 10 DPA	The individual to whom the information relates

any sensitive information which it has received by virtue of the Act.¹² The Regulations also prohibit disclosure of any sensitive information which the Category 1 or 2 responder has created in the course of discharging its duties under the Act.¹³ For example, a risk assessment might identify that a local authority's planning to evacuate a city centre was deficient, and would exacerbate the effects of a terrorist attack. Putting the information into the public domain could expose a weakness that might encourage an attack. If this information was obtained by virtue of an information request made under the Act, or created in the course of a Category 1 or 2 responder discharging its duties under the Act, the sensitive information must not be disclosed, even if it would otherwise fall within the Category 1 responder's duty to publish a risk assessment/plan or its duty to warn, inform and advise the public.

3.28 There are two exceptions in the Regulations to the prohibition on disclosure. Where the exceptions apply, the Category 1 or 2 responder may disclose. But unless the Category 1 or 2 responder is subject

to an obligation under the Act to disclose the information (eg as part of the obligation to publish risk assessments), it is not obliged to do so:

- **Consent for the publication or disclosure is obtained.** Consent should be obtained from the person identified in Figure 3.1. Note that the consent may be given subject to conditions.¹⁴
- **The information is commercially sensitive or personal data, but the public interest in disclosure outweighs the interests of the person or organisation concerned.** This exception does not apply if the information is sensitive by virtue of its national security or public safety implications. When relying on this exception, the Category 1 or 2 responder must inform the person or organisation to whom the information relates of its intention to disclose the information and provide reasons why it is satisfied that the public interest in disclosure outweighs their interests.¹⁵

3.29 The prohibition on disclosure only applies when the Category 1 or 2 responder is discharging its

¹² regulation 51(1)

¹³ regulation 51(5)

¹⁴ regulation 51(2)

¹⁵ regulation 51(6)

duties under the Act or any other function that it has in relation to an emergency. However, note that the restrictions on the use of information mean that in most cases sensitive information should not be used for other purposes. The prohibition does not apply where a Category 1 or 2 responder is dealing with an information request or contributing to the Community Risk Register (CRR).¹⁶

3.30 The prohibition will not apply where the Category 1 or 2 responder receives an information request under the Freedom of Information Act 2000 or the Environmental Information Regulations 2004. In such circumstances, Category 1 or 2 responders must consider the relevant enactment to determine whether or not the information should be released. (The right to information under each of those enactments is subject to limitations on disclosure. In many cases they will apply to sensitive information; but Category 1 or 2 responders should consider each case on its merits.)

3.31 The Regulations¹⁷ deal with the sharing of risk assessments to form the CRR. Where the risk assessment contains sensitive information, the Category 1 or 2 responder need not provide that information to the CRR where it considers that to do so would impair the confidentiality of that information or compromise the information. Note that there is no obligation under the Regulations to publish the CRR in its entirety. It is possible for a Category 1 or 2 responder to contribute a risk assessment to the CRR on condition that its risk assessment is not published.

How the requirements of the Act and the Regulations may be carried out

3.32 This section outlines how the Government believes the duties described may best be carried out. It describes good practice. Category 1 responders must have regard to this guidance.¹⁸

Types of information

3.33 It may be helpful for Category 1 and 2 responders to think about their use of information

in the round, and consider how streams of information interact.

3.34 There are various types of information. Information may be suitable for some audiences, but not others. And the circulation of information can be limited to certain classes of organisation or individual.

3.35 It is important not to think of information as being either public or private. The picture is much more nuanced, with a spectrum which runs from limited-access information (even within organisations) through to information intended to be absorbed and understood by the public.

3.36 However, there are certainly controls on the free flow of information. Access is limited in a range of ways including physical access, restrictive markings, circulation lists, the 'need-to-know' principle and targeting particular audiences.

Category 2 responders

3.37 As with co-operation obligations, it is important for Category 1 responders to be realistic about what information is requested from Category 2 responders. Information sharing has the potential to be very burdensome if it is not handled responsibly.

3.38 Category 2 responders often put information about their activities into the public domain. Information about the overall regulatory regime for Category 2 responders such as the utility and transport sectors is also widely available. In the first instance, Category 1 responders should seek information about the civil protection arrangements of Category 2 responders from these open sources. To facilitate this, the Government will work with Category 2 responders to put as much information as practical about their industry's civil protection arrangements into the public domain.

3.39 Beyond these generic arrangements, Category 1 responders can generally expect to be making information requests in a limited number of areas:

- information about local configuration of national arrangements;
- information about specific local facilities; and
- contact details of key staff.

¹⁶ regulation 51(1)

¹⁷ regulation 15(3)

¹⁸ s. cfp.283(3)(b)

3.40 Of course, this list is not exclusive. If a Category 1 responder wants information in order to discharge its duties under the Act it should approach the Category 2 responder in question and begin a dialogue about access. If that is not possible, or is unsuccessful, and the Category 1 responder believes the request to be reasonable and appropriate, it should make the request in accordance with the procedures set out in Annex A.

3.41 Where possible, Category 1 responders should seek to channel requests through as small a number of routes as possible so as to avoid duplication of effort. There are several ways in which Category 1

responders can request access to information to make the process more efficient:

- Where the information is required by a number of Category 1 responders, the request may be co-ordinated through the Local Resilience Forum (LRF), with the information shared between LRF members if appropriate. This is particularly relevant if the questions relate to local arrangements.
- Across a region, the request could be co-ordinated through the Regional Resilience Forum.
- Where a type of information request comes up repeatedly, a Category 1 responder should consider raising this with its national representative body, or the sponsoring government department, or

Box 3.1: The Government's protective marking system

One of the most common systems for the protection of documents is the Government's own document classification regime. The classification system is designed to protect valuable property or information, by labelling it with classifications, also known as protective markings. The system is operated by Government, and is linked to vetting overall security policy. As such it is not readily transferable to the local level, and should not provide the basis for any form of universally applicable system. And it should also be noted that even highly classified material may not be exempt from FOI requests. But it will be used by some Category 1 and 2 responders. There are four classifications:

- Restricted
- Confidential
- Secret
- Top Secret.

These classifications relate to the level of protection needed for the property or document. This operates on a sliding scale, and is based on:

- the damage that would be caused if it were lost, stolen or seen by an unauthorised person; and
- the subject of the document.

For example, loss of a Restricted document might cause distress to individuals or reveal confidential third-party information, whereas loss of a Top Secret document might cause very serious damage to UK armed forces or severe long-term damage to the UK economy.

The classification determines who can see the property or information, how it is stored and how it is transported or sent. But it should be noted that each item is classified on its own merits, and so it is not possible to say that all examples of a particular type of document – for example, an emergency plan – would be classified at a particular level.

In relation to access, classified documents are far less inaccessible than many people believe:

- To access Restricted information, you do not necessarily need any clearance but, in some cases, you may need a counter terrorist check (CTC).
- To access Confidential information, you may only need a basic check (BC). In some cases you may also need a CTC or a security check (SC).
- To access Secret information you must have an SC.
- To access Top Secret information you must have developed vetting (DV) clearance. But in some cases you may only need SC.

Category 1 and 2 responders should be willing to challenge organisations which over-classify material, or demand unwarranted levels of clearance.

through the national representative body for the Category 2 sector in question. This will allow the sector to consider whether adjustment might be made to the scope of publicly available information to remove the need for future requests.

3.42 In terms of sensitive information, most Category 2 responders are particularly likely to rely on exceptions that relate to commercial confidentiality. This reflects the fact that many of the Category 2 responders are private sector bodies, who may be in competition with other Category 2 responders within the same area. It is important that these needs are respected. For example, two mobile phone operators in the same LRF area might not want to expose details of their network coverage to each other, or to the public.

3.43 This would obviously be less true of those Category 2 responders from the public sector.

3.44 Category 1 responders should also bear in mind that information may be available to their organisation by virtue of existing commercial relationships with a Category 2 responder, or that information might be shared under the Act which would affect a commercial relationship. For example, an electricity supplier might have a contract to supply a local authority, but civil protection work might reveal problems with the resilience of that supply.

3.45 It is important that Category 1 responders respect the circumstances under which such information is obtained, and abide carefully by any restrictions on its use. Should Category 1 responders not handle information properly, the sanctions set out in the Act¹⁸ would be available to the Category 2 responder in question. In addition, Category 1 or 2 responders may also be able to rely on the law of confidence. In practice, any Category 1 responders acting inappropriately would be likely to receive additional advice from central government departments or Regional Resilience Teams.

3.46 In return for responsible use of these powers to request information, Category 2 responders should ensure that they can deal with reasonable requests made by Category 1 responders.

Other legislative requirements

3.47 Although there are many pieces of legislation which affect the use of information within individual sectors, there are three which have a wider-ranging impact and of which, as a consequence, Category 1 and 2 responders should be aware. It is for each Category 1 or 2 responder to make the final judgements about the detailed implications of each of these pieces of legislation and how they interface with the Act.

Freedom of Information Act 2000

3.48 The Freedom of Information Act 2000 (FOIA) provides a mechanism by which members of the public can access information held by public sector bodies.

3.49 The FOIA aims to increase the transparency of public bodies and the way in which such bodies carry out their work, and to increase accountability. For Category 1 and 2 responders which are Public Authorities as defined by the FOIA – broadly speaking that is a UK-wide public authority or a public sector body in England, Wales and Northern Ireland (similar legislation exists in Scotland) – the FOIA imposes certain duties to communicate information which is requested by any person (subject to procedural requirements and exemptions). These duties are not affected by the Act.

3.50 Although as a matter of law the FOIA could be used by one Public Authority to extract information from another, the FOIA is not primarily intended to be used for that purpose. Public Authorities have an implicit duty of co-operation in the discharge of public functions which should facilitate information flow. As such, Public Authorities which are Category 1 and 2 responders should not regard the FOIA as the principal basis for making requests from each other about civil protection matters. And Category 2 responders which are not Public Authorities should also not rely on the provisions of the FOIA as the principal basis to acquire information for civil protection purposes.

3.51 Instead, Category 1 and 2 responders should follow the two-stage process set out in earlier paragraphs. In the first instance, they should consider

¹⁸s. 10

whether it is possible to get the information they seek through other means.

3.52 It is only if the information is not publicly available that Category 1 or 2 responders should seek to use the formal mechanisms set out above. But this remains a last resort.

3.53 In most respects, the information-sharing provisions in the Act and Regulations are broader than those in the FOIA. The FOIA recognises that the information will enter the public domain. The Act recognises that the information stays within the civil protection community. As a result, the Act allows certain types of sensitive information to be shared which would be unlikely to be disclosed under FOIA.

3.54 Detailed guidance on the FOIA can be found on the Department for Constitutional Affairs website at <http://www.dca.gov.uk/foi/guidance/index.htm>

Environmental Information Regulations 2004

3.55 The Environmental Information Regulations 2004 provide for the freedom of access to information on the environment, subject to certain conditions, and must be taken into account when carrying out duties under the Act and Regulations.

3.56 Further information is available through the website of the Department for the Environment, Food and Rural Affairs, at <http://www.defra.gov.uk>

Data Protection Act 1998

3.57 The Data Protection Act 1998 provides certain rights to individuals to request information from public bodies about personal data held by them which relates to that individual. It also provides limits on the use or processing of such data by public authorities. The Data Protection Act must be considered in relation to the duties imposed under the Act and Regulations.

3.58 Guidance on the Data Protection Act can be found on the Information Commissioner's website at <http://www.informationcommissioner.gov.uk>