



**CabinetOffice**

# Information Sharing Under the Civil Contingencies Act 2004

Draft Revision to *Emergency Preparedness*,  
Chapter 3 (Information Sharing)

**Civil Contingencies Act Enhancement Programme**  
January 2010

## Contents

Introduction .....	3
Consultation Details .....	4
Purpose .....	4
Timetable .....	4
How to respond .....	4
Confidentiality .....	4
Background .....	5
Civil Contingencies Act 2004 .....	5
Civil Contingencies Act Enhancement Programme .....	5
Updating the Guidance .....	7
Evaluation of the existing guidance .....	7
Related proposals to take forward .....	7
Consultation, next steps and delivery .....	8
Annex A: Consultation Response Form .....	9
Annex B: Draft Revision to Emergency Preparedness, Chapter 3 (Information Sharing) ..	10

# Information Sharing Under the Civil Contingencies Act 2004

## Consultation Paper

### Introduction

1. The Cabinet Office is conducting a review of Part 1 of the *Civil Contingencies Act (2004)* (“CCA”), the *Civil Contingencies Act 2004 (Contingency Planning) Regulations 2005* (“the Regulations”) and the statutory guidance, *Emergency Preparedness*. We are delivering this review through the CCA Enhancement Programme. Phase 1 of the programme includes a specific project: *Information Sharing*.
2. The project sought to identify ways to improve information sharing between all Category 1 and Category 2 responders. As part of this project we identified a need to review Chapter 3 of *Emergency Preparedness* (Information Sharing).

## Consultation Details

### Purpose

3. The purpose of this consultation paper is to invite comments on the draft revision to Chapter 3 (Information Sharing) of *Emergency Preparedness*. This paper also explains the reasons for updating the current guidance and highlights the areas where key changes are proposed.

### Timetable

4. The consultation will run for eight weeks from 4 January 2010. We will consider all responses received by **26 February 2010**.

### How to respond

5. A separate response form accompanies this paper ([Annex A](#)). Please complete this form when responding to the consultation and send to: **ccact@cabinet-office.x.gsi.gov.uk** marking your response with 'CCAEP Information Sharing' in the subject field of your email.
6. Should you require this document or the consultation response template in a different format, please advise us of your specific requirements:
  - email: [ccact@cabinet-office.x.gsi.gov.uk](mailto:ccact@cabinet-office.x.gsi.gov.uk)
  - telephone: 0207 276 5017

### Confidentiality

7. We may pass the information you send to us to colleagues within Cabinet Office. We may also publish your comments in a summary of responses to this consultation. We will assume you are content for us to do this and, when replying by email, your consent overrides any confidentiality disclaimer that is generated by your organisation's IT system unless you specifically include a request to the contrary in the main text of your response to us.

## Background

### Civil Contingencies Act 2004

8. Part 1 of the *Civil Contingencies Act (2004)* (CCA) establishes a statutory framework of roles and responsibilities for organisations involved in civil protection at the local level. It creates two categories of responders and places a different set of duties on each. In England and Wales, Category 1 responders include local authorities, emergency services, health bodies and the Environment Agency. Category 2 responders include utility companies, transport operators and the Health and Safety Executive.
9. The main civil protection duties fall on Category 1 responders and these are:
  - risk assessment;
  - business continuity management;
  - emergency planning; and
  - maintaining public awareness and arrangements to warn, inform and advise the public.
10. A fifth duty applies to local authorities alone: provision of business continuity advice and assistance to the commercial sector and voluntary organisations.
11. Two further duties, co-operation and information sharing, apply to both Category 1 and Category 2 responders, and these facilitate local level partnership working between responders. The *Civil Contingencies Act 2004 (Contingency Planning) Regulations 2005* establish the Local Resilience Forum, the principal mechanism for multi-agency resilience work. Guidance for arrangements at the regional level is outlined in chapter 17 of *Emergency Preparedness*, the statutory guidance that accompanies the CCA.
12. The majority of Part 1 duties came into force in November 2005, with the exception of the local authority duty to promote business continuity which came into force in May 2006. Further details on the CCA and associated regulations and guidance can be found at:  
[www.cabinetoffice.gov.uk/ukresilience/preparedness/ccact.aspx](http://www.cabinetoffice.gov.uk/ukresilience/preparedness/ccact.aspx)

### Civil Contingencies Act Enhancement Programme

13. In March 2008, the Government announced a review of the CCA in the *National Security Strategy*. This was consistent with Government's earlier statement of intent made during the development of the Civil Contingencies Bill in 2003-04. The timing of the review, three years

after implementation, is consistent with wider Government policy on the periodic review of legislation to ensure statutory arrangements are fit for purpose.

14. Evidence from independent reviews and findings from the 2008 National Capabilities Survey indicate that implementation of the CCA has been largely successful and that it has made a significant contribution to enhancing emergency preparedness in the UK. However, during the initial stages of this work, evidence emerged, including findings from reviews of recent emergencies, which indicated that there are a broad range of CCA areas that would merit a more thorough review. The CCA Enhancement Programme was therefore established to deliver a number of policy projects through four phases to address the following objectives:
  - i. assess whether there are aspects of the CCA where original intentions are not being met and develop solutions where these are needed;
  - ii. consider whether the CCA needs to be modified to reflect relevant experience and changes in relevant structures which have emerged since the CCA came into force;
  - iii. consider how to reflect best practice in the CCA regime and supporting guidance to help raise the standard of UK resilience activity;
  - iv. evaluate whether the scope of the CCA should be broadened beyond emergency preparedness to cover the remaining aspects of integrated emergency management not already covered in Part 1; and
  - v. ensure that the CCA framework is effectively aligned and integrated with relevant legislation and policy initiatives.
  
15. The first phase of the programme focuses on improving the standard and consistency of implementation of the existing CCA framework. In line with objectives i and iii, this consultation proposes a revised version of Chapter 3 (Information Sharing) of the statutory guidance, *Emergency Preparedness*.
  
16. Further information on the programme can be found at:  
<http://www.cabinetoffice.gov.uk/ukresilience/preparedness/ccact.aspx>

## Updating the Guidance

17. The revised guidance aims to ensure that Chapter 3 (Information Sharing) of *Emergency Preparedness* provides an appropriate framework for responders to operate within. The guidance was developed in conjunction with a task and finish group, which had representation from Category 1 and Category 2 responders as well as government departments.

### Evaluation of the existing guidance

18. Whilst the task and finish group broadly endorsed the existing Chapter 3 and the guidance, [\*Data Protection and Sharing – Guidance for Emergency Planners and Responders\*](#), there was a concern that responders were not fully aware of the available guidance and were interpreting it differently. The task and finish group also identified a need to enhance the guidance on protective markings, security vetting, Data Protection and Freedom of Information, exercising and testing information sharing and LRF level information sharing protocols.

### Key changes proposed

19. Chapter 3 of *Emergency Preparedness* has been revised in part. The key changes proposed are:

- Greater emphasis on the benefit of Information Sharing protocols.
- The role of LRFs and RRFs in co-ordinating Category 1 requests for information from Category 2 responders.
- Clarification of Category 2 responders' duty under the CCA to share information about vulnerable people.
- A section on storing information.
- A section on exercising and testing information sharing.
- Stronger links with Chapter 2 (Co-operation) of *Emergency Preparedness* and the document, *Data Protection and Sharing – Guidance for Emergency Planners and Responders*.

### Related proposals to take forward

20. We have also been exploring options to improve training through awareness raising workshops which would include information sharing and protocols. Further information will be provided once the scoping exercise is complete.

## **Consultation, next steps and delivery**

21. The consultation questions are detailed in the response form which is attached as a separate document ([Annex A](#)). The questions refer to the draft revised guidance ([Annex B](#)).
  
22. Responses to this consultation will inform the final version of the revised chapter 3 (Information Sharing) of *Emergency Preparedness*. We anticipate publishing this in Spring 2010.

# Annex A: Consultation Response Form

Page left blank intentionally. Consultation response form provided as separate document.

## Annex B: Draft Revision to Emergency Preparedness, Chapter 3 (Information Sharing).

*Additions to the existing chapter are highlighted in blue.*

### 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 (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 3.8–3.12).
- 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 3.21–3.37).
- 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 3.56–3.68).
- Category 1 and 2 responders need to understand the importance of training and exercising information sharing elements of emergency plans to ensure they are effective (paragraphs 3.53-3.55).
- Further guidance on information sharing and data protection is available (paragraphs 3.69-3.70).

## 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 LRFs and RRFs, 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 as represented in Annex A of Chapter 2 (Co-operation)<sup>1</sup>. These are :

---

<sup>1</sup> This refers to a new table in the draft revision of Chapter 2 (Co-operation) of *Emergency Preparedness*.

- 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 the 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.

### **Devolved administrations**

**3.7** The way in which the information sharing duty under the Civil Contingencies Act 2004 applies to Category 1 and 2 responders in Scotland, Wales and Northern Ireland is much the same as in England. The key points in relation to the information sharing duty are:

- in Scotland, Part 1 of the Civil Contingencies Act 2004 (which includes the disclosure of information provision under which the Regulations were made) applies to Scotland, with the powers it sets out residing with Scottish Ministers<sup>2</sup>;
- in Wales, arrangements under Part 1 of the Civil Contingencies Act 2004 apply; and
- in Northern Ireland, duties in the Civil Contingencies Act 2004 apply only to a limited number of organisations which deliver functions which are not transferred (namely the Police Service of Northern Ireland, the Maritime and Coastguard Agency and telecommunications operators).

---

<sup>2</sup> Part 8 of the Civil Contingencies Act 2004 (Contingency Planning) (Scotland) Regulations 2005 (SI2005/494).

Where relevant, LRFs should be aware of the different structures in place and consider cross boundary information sharing requirements.

### **When information should not be formally requested**

**3.8** 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.

**3.9** The Regulations require Category 1 and 2 responders to consider alternative routes before pursuing a formal information request.<sup>3</sup> 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.

**3.10** 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.

**3.11** 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).

**3.12** 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. To assist the process LRFs are strongly advised to develop Information Sharing Protocols. These should recognise any pre existing organisational relationships and will include many of the informal information-sharing agreements that exist at the local level. Category 1 and 2

---

<sup>3</sup> regulation 47(3)(b)

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**

**3.13** 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<sup>4</sup>. 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

---

<sup>4</sup> regulation 47

order to make the system work.

**3.14** 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.”<sup>5</sup>

**3.15** Where the information is required by a number of Category 1 responders, the request may be co-ordinated through the LRF. In addition the Regional Resilience Forum (RRF) may facilitate the co-ordination of such requests from across the region. In Wales, this role is undertaken by the Wales Resilience Forum (WRF). This co-ordinated approach to information sharing should reduce the burden on those agencies from whom information is requested.

**3.16** Where there is a need to invoke a more formal approach for requesting information, a full explanation of the procedures to follow is set out in Annex 3A.

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

**3.18** A flowchart of key principles for

---

<sup>5</sup> regulation 47

information sharing is set out in Annex 3C.

## Storing Information

**3.19** Category 1 and 2 responders should also be aware of the differences required in handling personal data, when compared to handling sensitive security-related or commercial information.

**3.20** It is essential that Category 1 and 2 responders who request information formally or informally have appropriate methods of secure storage when the requested information is received. Each agency should have a locally defined protocol for handling, accessing, and storing information, especially that which relates to sensitive information.

### Exception to the duty in relation to sensitive information

**3.21** 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 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<sup>6</sup>. 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, National Criminal Intelligence Service

---

<sup>6</sup> regulation 45(1)

or Serious Organised Crime Agency), 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<sup>7</sup>.

**3.22** There are four different kinds of sensitive information as defined by the Regulations<sup>8</sup>:

- **Information prejudicial to national security** –

information, where disclosure to the public would adversely affect national security.

- **Information prejudicial to public safety** –

information, where disclosure 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, where disclosure 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), where

disclosure to the public would breach any of the data protection principles or section 10 of the DPA.

**3.23** 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

---

<sup>7</sup> regulation 49(4)

<sup>8</sup> regulation 45(1)

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<sup>9</sup>.
- 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.)

## **Using non-sensitive information**

### **Use within the planning process**

#### **3.24** The Act and Regulations do not

---

<sup>9</sup> regulation 46

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.

**3.25** 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**

**3.26** 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.

**3.27** 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),<sup>10</sup> the Freedom of Information Act 2000 and the Environmental Information Regulations 2004.<sup>11</sup>

## Using sensitive information

### Use within the planning process

**3.28** 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<sup>12</sup>. 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.

**3.29** 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.<sup>13</sup>

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

**3.31** 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.

---

<sup>10</sup> s. 2(1)(f)

<sup>11</sup> S.I.2004/3391

<sup>12</sup> regulation 52(1)

---

<sup>13</sup> regulation 52(2)

## Disclosure

**3.32** The Regulations prohibit any Category 1 and 2 responder from publishing or otherwise disclosing any sensitive information which it has received by virtue of the Act.<sup>14</sup> 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<sup>15</sup>. 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.

**3.33** 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.<sup>16</sup>
- **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.<sup>17</sup>

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

---

<sup>14</sup> regulation 51(1)

<sup>15</sup> regulation 51(5)

---

<sup>16</sup> regulation 51(2)

<sup>17</sup> regulation 51(6)

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).<sup>18</sup>

**3.35** 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 (bearing in mind that the presumption under FOIA is that all information will be disclosed). (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.)

**3.36** The Regulations<sup>19</sup> 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.

---

<sup>18</sup> regulation 51(1)

<sup>19</sup> regulation 15(3)

**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 <b>national security</b> 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 <b>national security</b> 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 <b>public safety</b> 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 <b>public safety</b> 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 <b>business or other affairs</b> 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

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

**3.37** 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.<sup>20</sup>

### **Types of information**

**3.38** 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.

**3.39** 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.

**3.40** 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.

**3.41** 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.

---

<sup>20</sup> s. 28 3(3)(b)

### Box 3.1: The Government's protective marking system and security vetting

There are various types of information. Information may be suitable for some audiences, but not others. Circulation of information may be limited to a certain category of organisation or individual. Whilst it is important not to think of information as being public or private, it needs to be remembered that there are controls on the free flow of information.)The non statutory guidance **Security Vetting and Protective Markings: A guide for Emergency Responders**<sup>21</sup> provides an overview of government policy for protective security and describes the protective marking system that is used by government. Category 1 and 2 responders should follow the relevant procedures outlines in the document.

#### Protective Marking

There are 6 key points for protectively marking material. These are:

- Not Protectively Marked
- Protect
- Restricted
- Confidential
- Secret
- Top Secret.

The large range of information that can be covered by PROTECT means that a descriptor should be used e.g. "PROTECT - FOR LOCAL RESILIENCE FORUM USE ONLY". Material which contains sensitive personal data should be marked "PROTECT – PERSONAL DATA". The non statutory guidance document describes the classification for each heading. It is however unlikely that responders will have a frequent need to work with highly classified material, but nevertheless, should understand the classification for each heading.

#### Security Vetting.

There are three types of personnel security controls (vetting levels) that affect access to protectively marked information. These are:

- **Baseline Standard (BS)** – previously known as Basic Check (BC) and also known as Baseline Personnel Security Standard. (BPSS). This standard may enable those who

---

<sup>21</sup> Currently only available on a restricted basis through Government Offices. We anticipate that an updated version will be made available on the National Resilience Extranet.

are cleared to have access up to CONFIDENTIAL and occasional controlled access to SECRET material.

- **Security Check (SC)** - This standard may enable those who have been cleared to have long term, frequent and uncontrolled access to SECRET information or assets; and occasional controlled access to TOP SECRET.
- **Developed Vetting (DV)** – This standard may enable those who are cleared to have long term, frequent and uncontrolled access to TOP SECRET information or assets.

It is essential that Category 1 and 2 responders assess the appropriateness of obtaining clearances for those staff attending emergency centres during incidents that are of a sensitive nature e.g. Nuclear, Terrorist (CBRNE) related incidents, where there may be a need to have access to sensitive information. In such prolonged incidents, relief workers who are brought into emergency centres to deal with sensitive incidents, should be in possession of the appropriate clearance which can allow access to CONFIDENTIAL, SECRET, TOP SECRET information as determined by the incident. Further detailed information can be found in the non statutory guidance which has been mentioned above. Category 1 and 2 responders should be willing to challenge organisations which over-classify material, or demand unwarranted levels of clearance.

## Category 2 responders

**3.42** 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.

**3.43** 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. RRFs may facilitate this role. (paragraph 3.15 also refers.)

**3.44** Whilst Category 2 responders do not have the same planning duties as Category 1 responders, Category 2 responders do have a duty to provide information when requested by another responder<sup>22</sup> if the responder

requires it:

- a) to perform its duties under the CCA; or
- b) in connection with the performance of another of its functions which relates to an emergency.

If a request is made, the Category 2 responder must, in principle, comply with the request. In addition to the exceptions discussed elsewhere in this chapter, the regulations prevent a Category 2 responder providing information if they consider that:

- a) the information requested is personal data;
- b) disclosure would contravene a data protection principle; or
- c) disclosure would be likely to adversely affect the confidentiality of the information.

In relation to information on vulnerable people, disclosure should not contravene a data protection principle. Provided that the requesting agency gives an assurance that the confidentiality in the information will not be breached, the Category 2 responder would be expected to provide the information as a general duty under the regulations.

---

<sup>22</sup> regulation 47 (1), 49 (1), 50 (1)

**3.45** 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.

**3.46** 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.

**3.47** 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 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.

**3.48** 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.

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

**3.50** 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.

**3.51** 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 Act<sup>23</sup> 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.

**3.55** 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.

### **Exercising (Validation, training and testing)**

**3.53** The regulations clarify the requirements in regard to the arrangements for exercises not only to ensure that emergency plans are effective, but also that training for Category 1 personnel and other persons whom the responder considers necessary should also be provided. In addition, whilst not all elements of the plan can be tested, crucial elements of the plan can. One of these elements is information management.

**3.54** It is vital that all Category 1 and 2 responders have an awareness of their roles and be reasonably comfortable with them before an incident occurs. Category 1 and 2 responders should receive awareness training in understanding and interpretation of the legislation relating to information sharing i.e. Data Protection Act 1998, Freedom of Information Act 2000, Environmental Information Regulations 2004. In addition lessons and experience from previous incidents

---

<sup>23</sup> s. 10

should also be included in any training and exercising of plans. Reference should be made to the use of national reports and recommendations from major incidents.

**3.55** Category 1 and 2 responders should regularly review their training and exercising programme to validate, exercise and test the information sharing and also interoperability of communications elements of an emergency plan. In undertaking such a review, it is essential that responders understand their role and can fulfil its purpose before an incident occurs. There are case studies available to assist Category 1 and 2 responders in exercising this element of the plan in the document, *Data Protection and Information Sharing Guidance for Emergency Planners and Responders*.

### **Other legislative requirements**

**3.56** 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**

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

**3.58** 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.

**3.59** 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.

**3.60** Instead, Category 1 and 2 responders should follow the two-stage process set out in earlier paragraphs. In the first instance, they should consider whether it is possible to get the information they seek through other means.

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

**3.62** 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.

**3.63** It is important however that RRFs/WRF and LRFs agree protocols for dealing with individual FOIA requests. This will ensure that the RRFs/WRF and LRF responders who receive the same individual FOIA

request from the public or media can produce a co-ordinated response to the request. The process may mean identifying a lead responder to deal with specific FOIA requests on behalf of the RRF/WRF or LRF responders bearing in mind what can and cannot be disclosed under the CCA.

**3.64** Detailed guidance on the FOIA can be found on the Ministry of Justice website at [www.justice.gov.uk](http://www.justice.gov.uk)

### **Environmental Information Regulations 2004**

**3.65** 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.

**3.66** 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**

**3.67** 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.

**3.68** Guidance on the Data Protection Act can be found on the Information Commissioner's website at:

<http://www.ico.gov.uk>

### **Other Related Guidance**

**3.69** *Guidance on Multi agency Interoperability* is available from

[www.npia.police.uk](http://www.npia.police.uk)

**3.70** *Data Protection and Information Sharing - Guidance for Emergency Planners and Responders* is available through the Cabinet Office website.

[www.cabinetoffice.gov.uk/ukresilience](http://www.cabinetoffice.gov.uk/ukresilience)

and *Security Vetting and Protective Markings: A guide for Emergency responders* is available on a restricted basis from regional resilience teams in Government Offices.

## **Annex 3A:**

### **Formal procedures for requesting information**

**3A.1** 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 responder” and “the receiving responder.”<sup>1</sup>

**3A.2** An information request should be made in writing. It must specify either the information required or a description of the information requested. The request should be sufficiently precise that the nature of the information sought is clear.

The request must include reasons as to why the responder needs the information.<sup>2</sup>

**3A.3** The request may specify a time limit for dealing with it, and the place at which the information should be provided. The request may also specify the form in which the information is to be supplied (e.g. in paper form, on disk). In each case, the time allowed and the place and form specified, must be reasonable. For example, a requesting responder seeking details from an established plan might allow a week for the receiving responder to reply. But if the information being sought is, for example, not presently collated in an easy-to-share way, or can only be released with the permission of a third party, a month might be more applicable. Wherever

possible, the mechanics of the request should be discussed in advance between responders.

**3A.4** A template for requesting information can be found at Annex 3B.

### **Procedure for dealing with a request**

**3A.5** A valid request for information in possession of the Category 1 and 2 responder receiving the request, must be complied with unless one of the exceptions applies. This is the case even where the information has been originally supplied in confidence – though the responder which receives the information is also likely to become subject to that duty of confidence. Where the responder is subject to restrictions on the disclosure of information in another enactment or a contract, the other enactment or contract will have to be considered in light of the Regulations.

Which provision applies will depend on the particular terms of the other enactment or contract.

**3A.6** In considering whether the request is valid, a responder should consider if the procedural requirements have been satisfied and whether the reasons given by the requesting responder indicate the information does appear to be reasonably required in connection with the requesting responder’s functions.

**3A.7** The information must be provided

within the time limit specified in the request. If no time limit is specified, the information must be provided in a reasonable period.

The information must be supplied in the form and at the place specified by the request.

**3A.8** The request relates to information, not documents. A responder which receives a request is not required to disclose all the documents which contain the information which has been requested. However, this will often be the easiest way to deal with an information request. In other cases, a new document which contains the information being requested may be prepared.

**3A.9** A template for responding to a request for information can be found at Annex 3B.

1 regulation 47

2 regulation 48

3 regulation 50

**Annex 3B:  
Information request proformas**

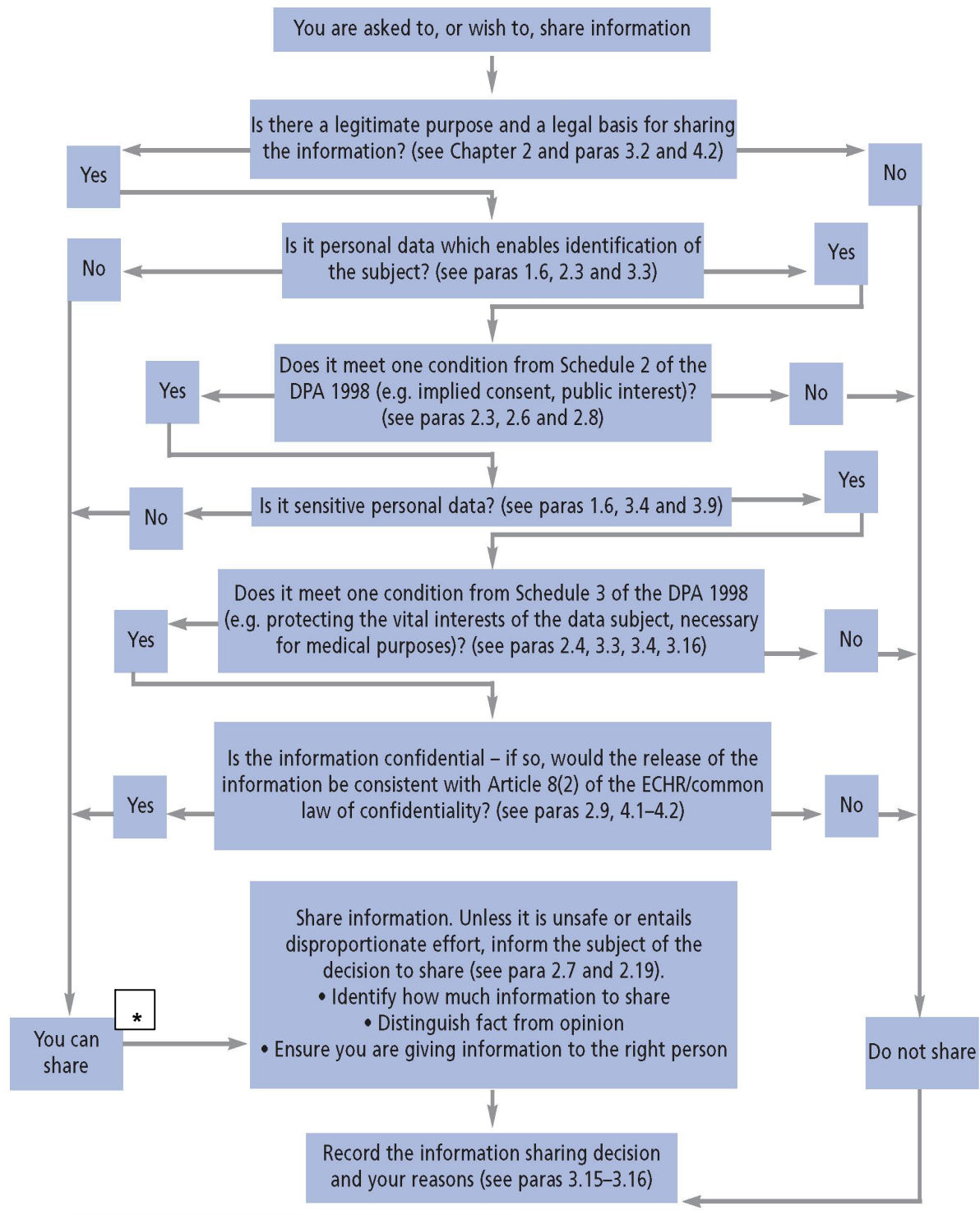
**Information request under the Civil Contingencies  
Act 2004**

Requesting organisation(s)	
Information holding organisation(s)	
Information requested	
Reason why the information is required in connection with the Act or other civil protection duties (and how the information is likely to be used)	
Date of request	
Date by which information is required	
Form in which information is required	
Place to which information should be sent	
Contact details	

**Response to information request under the Civil Contingencies Act 2004**

Requesting organisation(s)	
Information holding organisation(s)	
Date of request	
Information requested	
Request accepted?	Yes/no
If no, please set out the exceptions on which you are relying	
If yes, please set out any sensitivities or further background information which might be necessary to ensure the information is properly understood and properly protected	
Date information supplied	
Contact details	

## Annex 3C: Flowchart of key principles for information sharing



<sup>47</sup> Adapted from Information Sharing: A Practitioners Guide.

\* If the information is sensitive because it is information prejudicial to national security; to public safety; or is commercially sensitive information you should also consider whether this information should not be disclosed on those grounds. See paragraphs 3.21 to 3.23.