



CabinetOffice

Outline Specification for DHR Information Awareness Training.

Audience This paper will be of particular interest to:

- SIROs, IAOs and Learning & Development Units

Action

- Implement

Timing Immediate

Background

1. The data Handling Review states that Government will roll out at least a minimum level of information risk awareness training to all those with access to protected personal data to educate staff of the value of information and the potential threats to it.

Guidance

2. The guidance outlines the generic module structure, the core training specification the proposed delivery mechanism, methods of assessment, time frames for delivery and the role of departments and the centre in the delivery of training.

Contacts Enquiries about content should be directed to:
datareviewteam@cabinet-office.x.gsi.gov.uk

© Crown Copyright May 2008

Outline Specification for Information Risk Awareness training for all users of protected personal data in government

Purpose

1. This is an outline specification for internal or external developers of training packages for use by government departments and their delivery partners. This core specification assumes that the delivery mechanism is an e-learning package.

Background

2. In the light of the high profile data losses the Cabinet Office has undertaken a review of data handling procedures in government. As a consequence has stipulated that all government staff handling personal protected data must undergo training on appointment with an annual refresher.

Context

3. Every member of an organisation has their part to play in protecting information. This specification covers mandatory training for all departmental staff who handle, or are involved in managing, “protected personal data” in order to ensure that they understand its value and the potential implications of their actions. The definition of personal protected data is recorded at the end of this document.
4. This core training specification covers generic issues surrounding personal data handling. To make this training “real” departments should supplement it with local material based on their business needs. Departments should use the training as part of their structured plans to change behaviours across their organisation. The behaviours sought are ones where staff value, protect and use data for the public good.
5. Where departments have already developed, or are developing, their equivalent training, they should ensure that this covers all the outcomes and course content specified in this document.

Central Development

6. If required it may be feasible for the Cabinet Office, or another department acting on its behalf, to oversee the development of an e-learning package. This package

NOT PROTECTIVELY MARKED

would be delivered under a framework agreement accessible to government departments and other public sector organisations as required. The Cabinet Office invites comments from organisations as to their interest in access to a centrally-developed package.

7. Where departments and other organisations use their own training packages, they may wish to utilise some aspects of any centrally-provided package. The framework agreement should allow for full or partial provision to such organisations.

Audience

8. The training will apply to all staff regardless of grade and role that have, during the course of their duties access, or manage, protected personal data.
9. Departments should consider whether other staff (i.e. those who do not handle protected personal data) might also benefit from the training.

Delivery mechanism

10. Delivery should be by e-learning, supplemented by supporting materials to include local information (who to contact, where to find detailed guidance material etc) and ongoing periodic reminders of the need to be vigilant when handling protected personal data. The training should be designed so that the content may be supplemented as required with group awareness sessions to reinforce the message and as a means of highlighting particular local concerns.
11. The package should be modular with core and where necessary, a limited number of role-specific (e.g. manager or mobile worker) modules. All core modules will be mandatory.
12. It is anticipated that a centrally-developed package will use a portal approach so that departments may add modules themselves, or tailor pre-structured modules to their own needs by specifying their own scripts and scenarios. For example, in order to engage staff and allow them to properly understand the relevance of the training and the messages relevant to their particular roles, departments may wish to provide different example scenarios for different audiences, for example: staff dealing with benefits, family information, disabilities, and HR data. These

NOT PROTECTIVELY MARKED

scenarios should be used to portray the messages, the potential results of poor practice, and also in the assessment questions.

13. A centrally-developed package must be suitable to meet a wide range of internal network capabilities and local standards, including platforms, availability/non-availability of audio, and all accessibility requirements.

Maintenance

14. Materially for the core modules will be maintained centrally, so that departments can ensure that the content remains up to date and avoid duplication of effort and potential distortion of key messages.

Assessment

15. The package should provide a simple assessment process based on a multiple choice test, using selections from a bank of questions so that the same set of questions is unlikely to be repeated. The selection should include a given number of questions from each of several sets to ensure coverage of each key area.
16. Feedback should be given at the end of the assessment test, including a list of areas/modules to review where responses were incorrect.
17. Departments may wish to recognise successful completion, possibly by providing a certificate for those who successfully complete the assessment against an agreed pass mark. It shall be possible to maintain records of staff that have/have not completed the training and assessment so that line managers and individuals can be reminded and remedial action taken to help those who have not yet reached the pass mark.
18. Departments should be able to modify the questions to reflect any particular areas of general and local emphasis.

Generic module structure

19. All modules should have a consistent structure, to aid familiarity and ease of use. This will be:
 - Brief introductory sentence – perhaps with an eye-catching tabloid-style heading and some explanatory words giving an appropriate highlight (eg

NOT PROTECTIVELY MARKED

sensitive nature of information, consequences of getting it wrong)

- Module aim – what we will look at in this module
- Introduce subject and explain, using contextual examples as appropriate
- Questions to reinforce the message and bring out additional points, using contextual examples and with feedback on right and wrong answers
- Summary and any additional information

20. Relevant graphics should be used where this helps to reinforce the message and the context.

Supporting information

21. Departments may wish to provide staff with appropriate local supporting information, such as whom to contact in specific situations. Some of this information is unlikely to be standard even within a single department, but it either needs to be prominent and easily located on intranets (and signposted from the e-learning package) or provided as add-on information to any training package. The design of the e-learning package must therefore make the process of identifying and finding supporting information straightforward.

22. To reinforce the message and ensure the effectiveness of the training programme in changing staff behaviour, departments should ensure they have a planned programme of reminders (perhaps focussing on different topics at different times).

Timing

23. E-learning and assessment are to be completed during the induction period at the start of employment and when first moving into a role handling or managing protected personal data. Thereafter, it is to be annually refreshed, with an annual assessment.

24. For staff already in post, initial basic e-learning and assessment is to be completed, where feasible, within three months of the availability of training and not later than October 2009, as set out in the report of the Minimum Mandatory Measures.

NOT PROTECTIVELY MARKED

Information Risk Awareness Minimum Training Specification

25. Following training, the user will be able to demonstrate the following:

- Understanding of the value of information, and the different types of information they handle (personal information, anonymised person-based information, business information not about specific individuals);
- Personal responsibility for protecting the information with which they work and understanding of the implications for themselves if they do not protect that information;
- Understanding of the need to follow legal and corporate rules and good practice;
- Knowledge of appropriate techniques to protect information (including access control);
- Understanding of how their role supports corporate knowledge and information management.

Course content

26. The following should be included in the course (although some of these categories may be treated together rather than as discrete items of content):

- Definition of personal information, and other types of information (anonymised person-based information, business information not about specific individuals);
- Value of information, both to the business and to the original owners of the information (we are often just custodians of others' information), including information when brought together in bulk;
- Need to protect personal information and potential consequences of not protecting information:
 - Data Protection Act (including data handling principles);
 - Other legislation - Freedom of Information Act, Computer Misuse Act, Human Rights Act;

NOT PROTECTIVELY MARKED

- Risk to personal safety;
- Risk of crime;
- Financial loss (to individual and organisation);
- Damage to reputation, distress and inconvenience;
- Departmental policies and procedures.
- What is my responsibility? Why does it matter to me?
- What can I expect of my line management and others (e.g. Information Asset Owner);
- Responsibility of line managers (for those with line management responsibilities);
- Methods of keeping information safe (technological and procedural, including access control and passwords);
- The sharing and transfer of information within the organisation and others externally and the authority for such transfers;
- What are incidents and what should I do/where can I get help? (including anonymised reporting);
- Inappropriate behaviour and its potentially consequences to the individual (eg blatant disregard for processes designed to protect information).

26. Other topics which may be required in some, but not all, departments and public bodies, or for particular groups of staff (eg HR staff, home workers) are listed below (note that this list is not exhaustive):

- Remote working and home working;
- Requirements for staff who travel frequently;
- Role of senior managers;
- Secure disposal of documents and media;

NOT PROTECTIVELY MARKED

- Storage/handling of discarded material;
- Handling protectively marked documents;
- Issues when managing and negotiating contracted services;
- Bogus callers;
- Police enquiries;
- Professional codes;
- Children's issues;
- Public interest disclosures;
- Consent issues, including mental capacity;
- Leaks;
- Investigative journalists.

Detailed material

1. Specific material on which to build the content will be available from a CSIA-led working group which will also explore the issues of IPR and resourcing. CSIA welcomes offers of support for this working group. We shall be setting the group up very shortly and will be sending a calling notice to this effect.

Minimum scope of protected personal data

Departments must identify data they or their delivery partners hold whose release or loss could cause harm or distress to individuals. This must include as a minimum all data falling into one or both categories below.

A. Any information that links one or more identifiable living person with information about them whose release would put them at significant risk of harm or distress.

1. one or more of the pieces of information which can be used along with public domain information to identify an individual	combined with	2. information about that individual whose release is likely to cause harm or distress
Name / addresses (home or business or both) / postcode / email / telephone numbers / driving licence number / date of		Sensitive personal data as defined by s2 of the Data protection Act, including records relating to the criminal justice system, and group membership

NOT PROTECTIVELY MARKED

birth [Note that driving licence number is included in this list because it directly yields date of birth and first part of surname]		DNA or finger prints / bank, financial or credit card details / mother's maiden name / National Insurance number / Tax, benefit or pension records / health records / employment record / school attendance or records / material relating to social services including child protection and housing
---	--	--

These are not exhaustive lists. Departments should determine whether other information they hold should be included in either category.

B. Any source of information about 1000 or more identifiable individuals, other than information sourced from the public domain.

This could be a database with 1000 or more entries containing facts mentioned in box 1, or an electronic folder or drive containing 1000 or more records about individuals. Again, this is a minimum standard. Information on smaller numbers of individuals may warrant protection because of the nature of the individuals, nature or source of the information, or extent of information.