Ministry of Defence

Owner: MOD Head of Profession for Statistics

Author: Defence Statistics

Issue date: February 2017

Ministry of Defence
Disclosure and Confidentiality Policy – Identifiable Survey Data

Purpose

1. We hold identifiable personal data collected from Ministry of Defence (MOD) Civilian and Armed Forces employees in surveys. We have an obligation to act ethically and safeguard the confidentiality of individuals. We must also be fully compliant with the Data Protection Act 1998 (DPA98[1]), and the Freedom of Information Act 2000 (FOIA).

2. We must adhere to the UK Statistics Authority Code of Practice for Official Statistics (Principle 5: Confidentiality). We must also comply with the United Nations Economic Commission for Europe Fundamental Principles of Official Statistics[2].

3. We must comply with JSP 440: The Defence Manual of Security, JSP400: Disclosure of Information, and JSP200: Statistics.

4. We must ensure that we do not inadvertently disclose the identities of people in our published statistics and thus potentially infringe their right to privacy under the Human Rights Act 1998, the DPA98, or in common law.

5. Data includes photographs, videos, and sound recordings, as well as words and numbers. Data may be held in manual form such as forms and letters or their electronic counterparts.

Defence Statistics Policy

6. We need to obey the law by protecting the privacy of the people and enterprises whose data we hold.

7. We obtain, hold and use personal data on the Armed Forces and civilian workforce and this is covered by the Secretary of State's entry in the Data Protection Register. We must not use the data for any purpose other than those stated in the Register.

[1] The Act applies only to living persons, but there is a residual duty of confidentiality in common law to deceased individuals.
[2] These can be found at www.unece.org/stats/archive/docs.fp.e.html

Purpose of Data – Informed Consent

8. All surveys and censuses undertaken by Defence Statistics (DS) are based on the principle of informed consent – participants must be made aware of why data are being collected in advance of completing and submitting the questionnaire, and the data must only be used for that purpose. Where data are to be linked to other data at individual level e.g. from HRMS or JPA, or data collected in earlier surveys, participants are to be made aware of which data will be linked and why prior to completing the questionnaire.

Confidentiality

9. Respondents to surveys and censuses must be made aware of how confidentiality will be maintained. According to Principle 5 of the Official Statistics Code of Practice arrangements should be sufficient to protect the privacy of individuals but not so restrictive that the practical utility of the statistics is unduly limited. Any variations to these arrangements (including for legal or public interest purposes) must be authorised in advance by the MOD Head of Profession for Statistics and the National Statistician. All authorisations for such variations must be published.

Storage, Analysis and Transmission of Identifiable Survey Data

10. Except as described in 11 and 12 below, identifiable survey data (including sample lists and individual responses) must only be held and analysed on the DS network or officially provided laptops with encrypted hard disk drives. Identifiable survey data must be stored only on network drives or on encrypted hard disks on officially provided DS laptops. Access to the survey data will be restricted to the DS Surveys team and DS Corporate Systems staff who administer the DS Network and the databases held on the network. Access will be controlled by means of permissions and MOD compliant passwords.

11. The distribution of survey questionnaires and the collection of survey responses is contracted to Acuity Computing Enterprise Technology (a:cet) Limited, Centre 500, 500 Chiswick High Road, London W4 5RG. A:cet must maintain security standards equivalent to those described in 10 above. Compliance will be audited by the DS Data Manager and the HIS Enabling Team Leader on a regular basis.

12. Identifiable AFCAS data will be shared with single Service researchers to enable additional analysis to be undertaken to develop and monitor the effectiveness of personnel policies. Prior to the provision of data a signed Data Access Agreement must be returned to DS listing the data to be provided, the purpose for which it will be used and the names of all persons with access to the data. This use must be consistent with the ethical approval for AFCAS. Data provided must only be used by the persons listed in the Data Access Agreement for the purpose listed in the agreement. Any breach of the agreement must be reported to the National Statistician.

13. All identifiable survey data must be treated as “protect personal” and managed accordingly. The DS procedure for the Transfer of Survey Data must be complied with whenever data are transferred: data transfer must be over secure MOD networks or by means of encrypted USB storage devices.

Defence Statistics Staff

14. All DS staff will sign a declaration that they understand the law and their responsibilities regarding data protection, before being allowed access to personal data (survey or administrative). DS staff must not misuse the systems to derive sensitive information about individuals. Any attempt to do so is a disciplinary offence.

15. Contractors and consultants are treated as if they were DS staff. Thus contractors and consultants retained by DS are DS's responsibility and similar 'need to know' restrictions should be placed on their access to personal data. Usually, their 'need to know' will be a lot less than for many DS staff with ongoing responsibilities.

Publication of Data

16. While DS may hold identifiable survey responses, confidentially must be maintained in all published results (including drafts released to customers) through the application of methods of disclosure control. Further information about the use of disclosure control is set out in 'MOD: Disclosure control and rounding policy'[1].

Requests for Data

17. Section 33 of the Data Protection Act 1998 permits DS to pass anonymised data to a third party for research purposes.

18. Where datasets are requested for research purposes, anonymised datasets will be made available subject to consent by the Data Owner.

19. Datasets must be anonymised by removal of any unique identifier and ensuring that it is not possible to identify any individual by cross tabulation of demographic data items in the dataset.

20. Prior to the release of any dataset a signed Data Access Agreement must be returned to DS listing the data to be provided, the purpose for which it will be used and the names of all persons with access to the data. Data provided must only be used by the persons listed in the Data Access Agreement for the purpose listed in the agreement. For student research projects the Data Access Agreement must also be signed by the academic tutor supervising the research. Any breach of the agreement must be reported to the National Statistician.

Data Owner and Custodians

21. The survey data are owned by the organisation commissioning the research. The Data Owner will decide who may access the data and receive analyses based on the survey data. The data owner is responsible for responding to Parliamentary Questions and FOI requests relating to the survey.

22. The Head of DS Surveys Branch is responsible for ensuring that this policy is complied with and the confidentially of identifiable survey responses is maintained. This responsibility takes precedence over requests and instructions from the Data Owner.

[1] Accessible at www.gov.uk/government/publications/defence-statistics-policies

23. The Head of DS Corporate Services & Development is the Information Asset Owner (IAO) responsible for the security and safe keeping of all of DS's data including the survey data held on behalf of the Data Owner. Any queries regarding the Information Assurance of the data held should be directed to the IAO.

24. For the purposes of the DPA98, the Ministry of Defence is a single legal entity and the Secretary of State for Defence is its Data Custodian.

Implementation

25. This policy takes immediate effect. Every person working on identifiable survey data in DS is expected to adhere to this policy.

Annex A

List of sensitive personal information items

26. Data items listed in this section are deemed 'sensitive' by DS and particular care should be taken not to reveal them directly or indirectly about an individual. Items marked with an asterisk (*) are defined as sensitive personal data relating to the data subject (individual) by section 2 of the DPA98.

a. Any data collected where a guarantee of confidentiality was given
b. Racial or ethnic origin*
c. Nationality
d. Political opinions*
e. Religious or similar beliefs*
f. Whether a member of a Trade Union*
g. Physical or mental health or condition, including disability status*
h. Sexual life*
i. Commission or alleged commission of an offence*
j. Proceedings in relation to an offence or an alleged offence or any sentence imposed by any court in relation to them*
k. Age
l. Marital status
m. Cause of death, where this is not a matter of public record[3]
n. Benefit claims history or entitlement
o. Photographs, videos or sound recordings in which individuals can be identified
p. Any other data whose disclosure would cause the data subject embarrassment or distress and which they could reasonably have expected to remain private

27. The following data items are not considered sensitive on their own:
a. Sex
b. Rank or grade
c. Whether working full-time or part-time

[3] Reporting causes of death as recorded on death certificates would not be disclosive, since death certificates can be obtained by the general public from the General Register office. However, reporting that someone has died of, for example, 'an AIDS related illness' when the death certificate showed only 'respiratory failure' would be disclosive, and the data should be protected in accordance with the common law duty of confidentiality. This is also done for the sake of surviving relatives.