Ministry of Defence

DCS Policy Directive

7.1.1 Data Protection

DCS Jul 24 v3.0

General

Authorisation	Head DCS
Senior Responsible Owner	AH SIS
Point of Contact	POLRA
Review Date	March 2026
Related Policy/Guidance	Human Rights Act 1998 Data Protection Act 2018 Freedom of Information Act 2000 MOD Information Assurance Maturity Model JSP 440: Defence Manual of Security JSP 441: Defence Records Management Policy and Procedures ACSO 2002: Army Warning and Reporting Point (WARP) Security Incident Reporting, Management and Investigation ACSO 2190: The Security of Personal and Mission Critical Information Defence Digital DPA18 Toolkit DCS Directive 7.1.2: Records Management

Introduction

1. For Data Protection and the Management of Information Assets, DCS is accountable to The Data Protection Support Team in the Information Directorate at Army HQ. It is bound by the Data Protection Act 2018 (DPA18) and within the MOD conforms to JSP 440 and ACSO 2190[1]. Supplementary direction is also received through the Information Assurance Maturity Model (IAMM)[2].

Aim

2. The aim of this DCS Policy Directive is to provide direction on the process and procedures to be followed by all DCS personnel to afford personal and mission critical data the correct level of protection. It provides a framework to ensure that information assets are assured by internal audit, inspection and review and that any weaknesses are identified and rectified appropriately. This Policy Directive should be read in conjunction with the direction for the normal processing and retention of all DCS records, laid out in DCS Policy Directive 7.1.2: Records Management.

[1] ACSO 2190

[2] This policy directive has been considered against the Public Sector Equality Duty and it has been concluded that it is compliant.

Scope

3. This Policy Directive applies to all DCS personnel including:

   a. 3rd Party Suppliers (3PS) with whom DCS has contracted and where the nature of the business involves the collection, storage and processing of personal data for which the MOD (Secretary of State) would be defined as the Data Controller, and

   b. Delivery Partners (DP) such as Service charities, with whom DCS shares personal data

4. It applies to all data formats equally including electronic and hard copy data.

Roles and Responsibilities

5. Correct management of our personal and mission critical information is key to understanding what data we hold and what mission critical assets we are relying on to deliver our outputs. Protecting and managing these vital assets is everyone's business and the Army Information Asset Register (AIAR), coupled with the policy and guidance in this DCS Policy Directive, enables the Chain of Command (CofC) to be assured that this is happening.

6. All staff within DCS have an enduring responsibility to comply with DPA18 and to protect and safeguard the personal information it stores and processes for all personnel. Our responsibility is to protect personal data as required by DPA18, and to ensure that personal data does not fall into the hands of those who may wish to exploit it. In the Act personal data is defined as 'any information relating to an identified or identifiable living individual who can be identified directly or indirectly in particular by reference to an identifier such as a name, an identification number, location data or an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.'

7. Terms of Reference with detailed responsibilities are listed within **Annex B** of ACSO 2190 and in JSP 440. Key data protection roles within DCS are as follows:

   a. Personal Information Risk Owner (PIRO): Head DCS

   b. Personal Information Risk Manager (PIRM): DCS HQ Business Manager

   c. Personal Information Asset Owner (PIAO): Within each School, Setting and discrete data set owner (People using personal data require a PIAO to protect access to it)

   d. IT Security Officer (ITSO) within each School and Setting

   e. System Security Officer (SSO) (MOD Schools): RC-DCS-SIS-ICT Sen Sys Eng Cyp2

   f. HQ DCS MODNET (Local Security Officer) LSO: RC-DCS-SIS-IDD ISO SO3

   g. HQ DCS Local Data Protection Advisor (LDPA): RC-DCS-SIS-IDD IM DPA USyO SO2

   h. Unit Security Officer (USyO): RC-DCS-SIS-IDD IM DPA USyO SO2

   i. Information Manager (iMgr): RC-DCS-SIS-IDD IM DPA USyO SO2

8. Personal Information Asset Owner (PIAO): Anyone within DCS who holds direct responsibility for the collection, maintenance and use of personal data held in a DCS owned Personal Information Asset (PIA) as identified in the DPIAs.

9. Managers at all levels must ensure that their staff are appropriately trained and are applying Info Assurance / DPA principles and practices.

10. All DCS personnel (regardless of role) are responsible for:

a. ensuring their mandated data/information handling training is current

b. checking that any information that they are responsible for or provide to, or on behalf of, the Army is accurate and up to date

c. understanding the Government Security Classifications (GSC) and handling personal data appropriately, in accordance with legislation and MOD policy

Principles

11. **Information Assets** Information is a key business asset, and its' correct handling is vital to the delivery of our services and the management of our personnel. Direction on the management of information assets is detailed in this document.

12. **Personal Data** Personal data must be protected as required by law under DPA18 and ensure that it does not fall into the hands of those who may wish to exploit it.

13. **Mission critical information** DCS is required to afford protection to our mission (or 'business') critical information. Mission critical information is taken to mean and include information that is indispensable to delivering the day to day running and business capability of any element of DCS.

14. **Subject Access Request (SAR)** Any request for personal data received from the data subject or their parent/legal guardian, is to be sent immediately to the HQ DCS Information Manager via the group mailbox (RC-DCS-HQ-MAILBOX@mod.gov.uk). Detailed instructions are provided at paras 23-25.

15. **Managing Data Breaches** Any breach, loss or compromise of personal data must be reported immediately. If you become aware of a data breach, loss or compromise of personal data, you must pass the details to the mailbox above and follow the direction at paras 35-41

16. **Assurance** Internal audit processes provide important assurance that the processes and procedures directed in this document are being followed and legal and mandatory requirements are being met. This requirement is a standing agenda item at Senior Leadership Meetings. Within DCS periodic assurance of compliance with DPA18, ACSO 2190 and this Policy Directive is conducted as below:

17. **DCS UK** Inspection of DCS HQ AIAR by the Army Data Protection Support Team (DPST)

a. **DCS Overseas** Other DCS elements are to conduct a self-assurance assessment at least annually, and report outcomes to the HQ DCS Data Protection Team, who will update the AIAR. These assessments are achieved through the annual review of the DPIAs and recording the evidence on each asset record on the AIAR.

Data Protection

18. DCS needs to collect and use certain types of personal data for the purposes of satisfying business and legal obligations. DCS recognises the importance of the correct and lawful use and treatment of personal data and the need for all personnel to recognise their individual responsibility to handle and protect personal information to meet the requirements of DPA18.

19. All DCS personnel who obtain, handle, process, transport and store personal information for DCS must adhere to these principles.

20. The overarching Army Data Protection Policy, guidance on the principles and exemptions to DPA18 are contained within ACSO 2190.

21. **Principles**: The 6 principles outlined below must be followed when obtaining, storing, processing, and disposing of personal data. The principles require that personal data shall:

a. **Principle 1**: Be processed fairly and lawfully and in a transparent manner

b. **Principle 2**: Must be collected for specific, explicit and legitimate purposes

c. **Principle 3**: Must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

d. **Principle 4**: Be accurate and, where necessary, kept up to date.

e. **Principle 5**: Must be kept in a form which permits identification of data subjects for no longer than is necessary

f. **Principle 6**: Personal data must be processed in a manner that ensures appropriate security of the personal data

22. **Personal Data**. All individuals who are the subject of personal data held by DCS are entitled to receive the following information:

a. The identity of the data controller

b. The identity of any representative of the data controller

c. The purpose(s) for which their data are intended to be processed

d. Any further information which is necessary to enable the processing in respect of the data subject to be fair[3]

23. **Subject Access Request**[4] If you receive a request for any type of personal information (SAR) you must pass the details to HQ DCS immediately to the mailbox above.

---

[3] 'Fairness' is not defined by DPA 18, however, anything that breaches the 6 principles can be defined as 'unfair'. Some examples of information that should be included to ensure processing is fair are: information on outsourcing or the use of Data Processors/Contractors; disclosures to third parties; additional information on the Data Subject's rights and all other information that is relevant to ensure transparency.

[4] Certain responsibilities apply to responding to SARs full guidance on how to progress them can be accessed at the Subject Access Requests section of the Army Data Protection website and the MOD DPA Toolkit

24. All individuals who are the subject of personal data held by DCS are entitled, subject to the provision of exemptions in DPA18 and outlined in ACSO 2190 to:

a. Be given by the data controller a description of the personal data of which they are the data subject

b. Be told the purposes for which their personal data is being (or will be) processed

c. Be provided with details of recipients, or classes of recipients, to whom their data may be disclosed

d. To have communicated to them in intelligible form the information constituting their personal data

e. Any information available regarding the source of their data

25. Within DCS any SAR received is to be forwarded immediately to DCS HQ Information Management Team via RC-DCS-HQ-IHUB@mod.gov.uk who will action without delay in accordance with 2018DIN05-016[5] to ensure that the data subject receives this information within one calendar month of making their request in accordance with DPA 18. Complex requests may be eligible for an extension of up to a further two calendar months.

26. **Data Security.** DCS recognises the need to ensure that personal data is kept secure during all aspects of processing in accordance with DPA 18, Principle 6. Personnel are to take all necessary steps against physical loss or damage, unauthorised access, and unauthorised disclosure. To this end, all personnel are responsible for ensuring that any personal data for which they are responsible is kept securely in accordance with ACSO 2190 (and JSP 440 and LFSO2008[6] – see Introduction).

27. Personal information is not disclosed either orally, in writing or otherwise to any unauthorised third party.

28. Personal information is not accessed by any unauthorised personnel.

29. **Electronic Filing.** To ensure that information stored electronically is appropriately secure it is essential that access to sensitive information is stored in a limited area of SharePoint, available only to those entitled to see it.

30. Relevant permissions on limited access sites must be set up correctly through the IHUB and checked at least annually by the IHUB on the direction of the PIAO for the container. This not only prevents unauthorised users accessing the sites directly, it also prevents anyone searching for data being shown the results of searches to sites where they do not have access. The AIAR entry for each personal data container must be updated annually by the PIAO.

31. **Retention of Data.** DCS will retain some forms of personal information for longer than others. All Information Asset Owners are responsible for ensuring that the information they are responsible for is not kept longer than necessary (for the purpose for which it was obtained), in accordance with DPA18 and the Human Rights Act 1998. In striking the right balance between

[5] 2018DIN05-016
[6] LFSO 2008

sharing and protecting information, we must continually manage business impacts and risks associated with the confidentially, integrity and availability of our information.[7]

32. **Identification, Ownership and Registration**. An information asset is defined as: 'A body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively'. Information assets have recognisable and manageable value, risk, content and lifecycles. An Information Asset:

a. is a repository of data that has value to the organisation, its business or operations and its continuity

b. supports a business/operational process

c. has longevity

d. is retrievable by others

e. is likely to harm the organisation or individual in some way (including reputational damage) if it is lost, compromised, or becomes unavailable to the business

f. has an owner (or owners) who is (are) responsible for its through-life maintenance

g. is not easily replaced without an impact on resources (costs, skills, time)

33. To provide the correct level of assurance to our information assets DCS are mandated to record the following data on the AIAR:

a. Personal Information Assets (PIA)

b. Mission critical information assets

c. Risk assessments and Data Protection Impact Assessments (DPIA)

d. Exemption certificates

e. Storage and processing of assets and the systems in use

f. IT Security Accreditation of systems in use

g. Personnel assigned to mandated protection/info governance roles and their training

h. Personnel assigned to all security roles and their training

i. A record of DPA training achieved for DCS personnel

34. HQ DCS will identify relevant PIA's and Mission Critical Information Assets within DCS and will direct the necessary action for registration on the AIAR, and whether there will also be a requirement for a DPIA, following the procedures detailed in ACSO 2190.

[7] See ACSO 2190

Breach Management

35. Anyone who discovers a breach, loss or compromise of personal data must raise and submit a Security Incident Reporting Form (SIRF)[8] [9] in accordance with JSP 441[10] immediately and contact the Army Warning and Reporting Point (WARP).

36. **Contact details for WARP** E-mail: ArmyWARP-Mailbox@mod.gov.uk Use Army Info-CyberSy-WARP.to search for team members on skype). The duty phone number is 01264 886804. The out of hours phone number is 07717424181.

37. The IHUB should also be contacted via RC-DCS-HQ-IHUB@mod.gov.uk who will notify Head DCS and DCS COS as soon as possible.

38. Guidance on the management of data breaches can be sought from Business Managers in MOD School Hubs.

39. A breach, loss or compromise of personal data may be the result of:

a. loss or theft of equipment or documents on which data is stored

b. inappropriate access controls allowing unauthorised use

c. human error

d. unauthorised disclosure

e. accidental destruction

f. hacking or targeted attack

g. unforeseen circumstances such as fire or flood

40. **Control** In the event of a breach, loss or compromise of personal data HQ DCS data protection and security staff will immediately implement the initial procedures contained within ACSO 2002 and ACSO 2190 which will include:

a. Identifying and appointing the most appropriate individual to act as Incident Manager

b. Identifying all stakeholders

c. Determining precisely what elements of personal data have been breached, lost or compromised

d. Identifying the circumstances leading to the incident to notify Army WARP via the SIRF

41. **Action.** Thereafter the Incident Manager will coordinate the following activities in accordance with ACSO 2002[11] and ACSO 2190:

---

[8] Security Incident Reporting Form
[9] Security Incident Reporting Form (SIRF) user guide
[10] JSP 441 Reporting a personal data Incident
[11] ACSO 2002

a. Make an immediate report to Army WARP as detailed above

b. Initiate Containment and Recovery actions

c. Assess the risk to Data Subjects and MOD reputation

d. Carry out required notification (informing Data Subjects)

e. Maintain the data protection breach management summary action table

Training

42. All DCS staff are to undertake and maintain training in accordance with Table 1 below. Where individuals do not have access to online training, HQ DCS will provide appropriate training materials. Detailed direction on training is accessed in ACSO 2190.

Training Course	Requirement
Protecting Personal Data [12]	**Mandated annually** To be completed by all Service Personnel, Civil Servants and Contractors who manage and handle information and who regularly access Defence Information Systems. New entrants to the MOD are to complete this training within 3 months.

Table 1 Training Requirements

43. **Training Records** For the MOD to provide assurance to the Information Commissioner, each Head in overall charge as PIRO (for DCS this is Hd DCS) is accountable and must be able to demonstrate their compliance. This is achieved through the annual completion and signing of the certificate of conformity, which lists thirteen requirements and includes the statement 'All personnel have completed a level of Data Protection training commensurate with their role'.

44. To enable this, all DCS elements will need to submit training compliance statistics to DCS SO2 DPA before the end of February each year, to meet the annual data harvest by Army HQ in March. DCS SO2 DPA will collate these statistics and report compliance annually through the AIAR.

45. All DCS branches are to retain electronic copies of training certificates issued to individuals on completion of mandatory training, either uploaded to your HR tool (MyHR/JPA) or held personally. These records are to be kept for the period that the certificate is valid, which is currently one year for Protecting Personal Data. Absence of a record at inspection or audit will be treated as evidence of non-completion of training and line managers will need to follow performance management procedures to address non-compliance.

[12] Link