Ministry of Defence

DCYP Directive 7.1.1

Data Protection Within DCYP

DCYP 7.1.1 Version 2.2 XXX19

General

Authorisation	Director DCYP
Senior Responsible Owner	DCYP Personal Information Risk Manager (PIRM)
Point of Contact	DCYP-DCYP-Mailbox@mod.uk 01980 61 8280 94344 8280
Review Date	XXX 2021
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 2190: Security of Personal and Mission Critical Information May 2017 DCYP Directive 7.1.2: Records Management

Introduction

1. This DCYP Directive is derived from, and remains subordinate to, **Army Command Standing Order (ACSO) 2190 (Security of Personal & Mission Critical Information)**. The direction contained in ACSO 2190 will **ALWAYS** take precedence over this DCYP Directive.

2. Although a MOD Directorate, DCYP operates within the Army TLB and thus conforms to Army policy, rules and guidance unless directed otherwise. For the purposes of Data Protection and the Management of Information Assets, DCYP is held to account by Army HQ, and conforms to Army Command Standing Order (ACSO) 2190 (which in turn conforms to JSP 440 (The Defence Manual of Security), which in turn conforms to the Data Protection Act of 2018 (DPA 18) and supplementary direction received through the Information Assurance Maturity Model (IAMM)).

KEY DIRECTION

- **Data Breaches**. If you become aware of a breach, loss or compromise of personal data you must pass the details to HQ DCYP (DCYP-DCYP-Mailbox@mod.gov.uk) immediately, and follow the direction at **Chapter 4**).
- **Subject Access Requests**. If you receive a request for any type of personal information you must pass the details to HQ DCYP (DCYP-DCYP-Mailbox@mod.gov.uk) immediately (details at Chapter 2, Paragraphs 23-25).
- **Freedom of Information Requests**. If you receive a request for any type of non-personal information you must pass the details to HQ DCYP (DCYP-DCYP-Mailbox@mod.gov.uk) immediately.

Aim

3. The aim of this DCYP Directive is to provide direction on the process and procedures to be followed by all DCYP 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 Directive should be read in conjunction with DCYP direction for the normal processing and retention of all DCYP records, laid out in Directive 7.1.2: Records Management which is accessed on DCYP SharePoint sites (including MOD Schools).

4. **This Directive is a stand-alone document which is derived from, and repeats essential elements of, ACSO 2190; but remains subordinate to ACSO 2190 under all circumstances.**

Scope

5. This Policy Directive applies to all DCYP elements and personnel. It also applies to:

a. Those 3rd Party Suppliers (3PS) with whom DCYP 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;

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

Roles and Responsibilities

6. Correct management of our personal and mission critical information is key to understanding what data we hold on our personnel 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 AIAR, coupled with the policy and guidance in this DCYP Policy Directive, will provide the Chain of Command (CofC) with the assurance that this is happening.

7. DCYP has an enduring responsibility to comply with DPA 18 and to protect and safeguard the personal information it stores and processes for all personnel. Our responsibility is twofold: we must protect personal data as required by law under DPA18; and we must ensure that personal data does not fall into the hands of those who may wish to exploit it. Personal information is defined as: data which relates to a living individual who can be identified:

a. From that data, or

b. From that data and other information which is in the possession of, or is likely to come into possession of, the Data Controller (the Secretary of State for Defence is the Data Controller for the MOD).

8. Terms of Reference with detailed responsibilities are listed within Annex D to ACSO 2190. Key data protection roles within DCYP are as follows:

a. Senior Information Risk Owner (SIRO): Dir CYP.

b. Personal Information Risk Manager (PIRM): AH Pol Plans, HQ DCYP.

c. IT Security Officer (ITSO):

d. MOD Schools Network: MOD Schools ITSO (Cyprus).

e. MODNet: SO3 ISO 1, HQ DCYP.

f. Data Protection Advisor: HQ DCYP SO2 Information Manager & DPA.

9. Personal Information Asset Owner (PIAO): **Anyone** within DCYP who holds direct responsibility for the collection, maintenance and use of personal data held in a DCYP-owned Personal Information Asset (PIA).

10. Managers at all levels must ensure that their staff are appropriately trained and are applying IA/DPA principles and practices.

11. All DCYP personnel (regardless of role) are responsible for:

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

b. Checking that any information that they 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/Army policy.

Principles

12. **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 Chapter 3 of this document.

13. **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.

14. **Mission critical information.** DCYP 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 DCYP.

15. **Subject Access Requests (SARs)**. Any request for personal data received from the data subject or their parent/legal guardian, is to be sent **immediately** to the HQ DCYP Information Manager via the group mailbox DCYP-DCYP-MAILBOX@mod.gov.uk. Detailed instructions are provided in Chapter 2 of this Directive.

16. **Managing Data Breaches.** Any breach, loss or compromise of personal data must be reported **immediately** in accordance with Chapter 4 of this Directive.

17. **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 all DCYP Command Groups. Within DCYP periodic assurance of compliance with DPA 18, ACSO 2190 and this Directive is conducted as below:

a. **DCYP UK.** Inspection of HQ DCYP by the Army DPST;

b. **DCYP Overseas.** Other DCYP elements are to conduct a self-assurance assessment at least annually, and report outcomes to Data Protection Advisor, HQ DCYP, who will update the AIAR. The HQ DCYP Data Protection staff will issue the question set for this self-assessment separately and may conduct the assessment in person.

Data Protection

18. DCYP needs to collect and use certain types of personal data for the purposes of satisfying business and legal obligations. DCYP recognises the importance of the correct and lawful treatment of personal data and the need for all personnel (regardless of their role) to recognise their individual responsibility to handle and protect personal information in order to meet the requirements of DPA 18.

19. DCYP fully adheres to the 6 principles of the Data Protection Act. All personnel (Military, Civilian, 3rd Party Suppliers (3PS) and Delivery Partners (DP)) who obtain, handle, process, transport and store personal information for DCYP must adhere to these principles.

20. The overarching Army Data Protection Policy is contained within **Annex A to ACSO 2190**.

21. **Principles.** As defined in DPA 18, personal data is: "Data which relates to a living individual who can be identified; from that data, or from that data and other information which is the possession of, or is likely to come into the possession of, the Data Controller[1] and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual". For the purposes of this Directive, the Data Controller is taken to mean the Army acting on behalf of the MOD.

[1] The Data Controller for the MOD is the Secretary of State for Defence.

22. There are 6 principles which 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 shall not be processed unless certain conditions are met.

b. **Principle 2**: Be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner that is incompatible with the original purpose.

c. **Principle 3**: Be adequate, relevant and not excessive for those purposes.

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

e. **Principle 5**: Not to be kept for longer than is necessary for that purpose.

f. **Principle 6**: Be processed in an appropriate manner to maintain security.

23. Guidance on the application of these principles is contained in **Appendix 1 to Annex A to ACSO 2190**.

24. Guidance on exemptions to DPA 18 is contained in **Appendix 2 to Annex A to ACSO 2190**.

25. **Personal Data**. All individuals who are the subject of personal data held by DCYP 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.[2]

26. **Subject Access.**[3] All individuals who are the subject of personal data held by DCYP are entitled, subject to the provision of exemptions at Appendix 2 to Annex A to 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;

---

[2] 'Fairness' is not defined by DPA 18, however, anything that breaches the 6 principles can be defined as 'unfair'. Aome of 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; additonal information on the Data Subject's rights and all other information that is relevant to ensure transparency.
[3] Full guidance on how to progress a SAR can be accessed at the Subject Access Requests on the Army Data Protection Website.

e. Any information available regarding the source of their data.

27. Within DCYP any Subject Access Request received is to be forwarded **immediately** to DCYP HQ SO2 Information Management and DPA via DCYP-DCYP-Mailbox@mod.gov.uk; who will action accordingly.

28. DCYP will make every effort to ensure that the data subject receives this information within one calendar month of making their request in accordance with DPA 18[4]. Complex requests may be eligible for an extension of a further one calendar month.

29. **Data Security.** DCYP 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:

a. Any personal data for which they are responsible is kept securely in accordance with **ACSO 2190** (and JSP 440 and ACSO 2008 – see Preface);

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

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

30. **Management of Data Breaches.** Any breach, loss or compromise of personal data must be reported in accordance with Chapter 4 of this Directive.

31. **Electronic Filing.** To ensure that information stored electronically is appropriately secure it is essential that access to sensitive information is limited to those entitled to see it.

32. Relevant permissions on limited access sites must be set up correctly and regularly checked. 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. It is important to note that file permission in MOSS do not transfer automatically to Meridio; they must be set separately.

33. **Retention of Data.** DCYP 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 DPA 18 and the Human Rights Act. Detailed direction on the retention of records is laid out in DCYP Directive 7.1.2: Records Management which is accessed on DCYP SharePoint sites.

Information Assets

34. Information is a key business asset and its correct handling is vital to the delivery of our services and the management of our personnel. In striking the right balance between sharing and protecting information, we must continually manage business impacts and risks associated with the confidentially, integrity and availability of our information.

[4] Certain responsibilities apply to responding to SAR. Guidance is accessed on the Army Data Protection website.

35. The overarching Army Policy on the Registration and Management of Information Assets is contained within **Annex B to ACSO 2190**.

36. **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).

37. To provide the correct level of assurance to our information assets the Army has developed the Army Information Asset Register (AIAR). DCYP are mandated to use the AIAR to record the following data:

a. Personal information assets;

b. Mission critical information assets;

c. Risk assessments and Privacy Impact Assessments (PrIA);

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/information governance roles and their training;

h. Personnel assigned to all security roles and their training;

i. A record of training achieved for DCYP personnel.

38. HQ DCYP will identify relevant Personal Information Assets and Mission Critical Information Assets within DCYP and will direct the necessary action for registration on the AIAR, and whether there will also be a requirement for a Privacy Impact Assessment (PrIA), following the procedures detailed in **Annex B to ACSO 2190**.

Breach Management

39. Any breach, loss or compromise of personal data must be reported **immediately** to HQ DCYP SO2 Information Manager via DCYP-DCYP-Mailbox@mod.uk

40. MOD school Business Mangers will provide guidance on the management of data breaches.

41. If the individual discovering the data breach is unable to contact HQ DCYP, they must contact the Army Warning Advice and Reporting Point (WARP) directly. Contact details for the Army WARP are:

SO2 WARPMil 94393 6804 Civ 01264 886804

SO3 WARP 1Mil 94393 7544 Civ 01264 887544

SO3 WARP 2Mil 94393 6804 Civ 01264 886804

Email: ArmyWARP-Mailbox@mod.uk

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

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/flood.

43. **Control**. In the event of a breach, loss or compromise of personal data HQ DCYP data protection and security staff will **immediately** implement the initial procedures contained within **Annex E to 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 inform the initial, IMMEDIATE report to Army WARP.

44. **Action.** Thereafter the Incident Manager will coordinate the following activities in accordance with **Annex E to ACSO 2190:**

a. Make an immediate report to Army WARP;

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

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

Training Course	Requirement
Defence Information Management Passport (DIMP)	**Mandated 3 yearly:** 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 MOD/Armed Forces are to complete this training within 3 months.
Responsible for Information **(Information Asset Owner) or (Senior Information Risk Owner) or (Non- Executive Director and Boards)**	**Mandated 3 yearly:** To be completed by all Service Personnel, Civil Servants and Contractors who manage and handle information, have regular access to Defence Information Systems and are employed as Information Asset Owners, Senior Information Risk Owners and Non-Executive Directors and Board Members. Training is to be completed commensurate with the role and within 3 months of taking up the post.

Table 1: Training Requirements

46. **Training Records.** For the MOD to provide assurance to the Information Commissioner, each Head of Establishment as Senior Responsible Owner (generally at Director level) 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".

47. To enable this, all DCYP elements will need to submit training compliance statistics to HQ DCYP Data Protection Advisor before the end of February each year, in order to meet the annual data harvest by Army HQ in March. HQ DCYP Data Protection Advisor will collate these statistics and report compliance annually through the AIAR.

48. All DCYP elements are to retain paper copies (or some other record such as a scanned copy) of certificates issued to individuals on completion of mandatory training. These records are to be kept for the period that the certificate is valid, which is currently 3 years for DIMP and 3 years for Responsible for Information. Absence of a record at inspection or audit will be treated as evidence of non-completion of training.