

1 Emergency and Disaster Planning

Contents

Title	Page
Introduction	1
Roles and Responsibilities	2
Developing Plans	4
Testing Plans	6
Retention of Records	6
Related Documents	7
Annex A – Outbreak management	A-1

Amendment Record

This chapter will be reviewed by the Health, Safety and Environmental Protection (HS&EP) Directorate together with relevant subject matter experts and key HS&EP stakeholders. Any suggestions for amendments should be sent to HSEP-GroupMailbox@mod.gov.uk.

Version No	Date	Text Affected	Authority
1.2	Oct 20	Interim update post-handover of Policy from DSA to D HS&EP.	D HS&EP
1.3	May 22	Updated to incorporate DAN 25 (Outbreak management) into Annex A.	D HS&EP

Introduction

1. This chapter provides guidance on the scoping, development and implementation of emergency and disaster planning. It provides the general principles and minimum planning requirements to be considered for possible emergency scenarios across the wide range of establishments, premises and capabilities (including vessels) where activities undertaken in Defence occur and require subsequent emergency planning. The related documents and regulations listed at the end of this chapter provide more detail in specific circumstances.

2. The Management of Health and Safety at Work Regulations requires Defence to risk assess its activities and to establish appropriate (emergency) procedures to be followed in the event of serious and imminent danger to Defence personnel and visitors, and the necessary contact required with external services (Ambulance, Fire, etc.). The Emergency and Disaster Plan should set out the information, procedures and details required to ensure an effective, flexible and timely response to an emergency, thus reducing to a minimum the distress and disruption caused by such an incident.

3. The purpose of emergency and disaster planning is to provide Defence personnel with the procedures, information and equipment they will require to enable them to ameliorate the effects of any major emergency occurring. A fast response to any emergency or disaster is essential to minimise injury or loss, therefore careful planning, training and emergency exercises are required to ensure that appropriate assistance is provided as quickly as possible.

4. In the event of an emergency or disaster, the preservation of safety and / or health of personnel will depend on their knowledge of whom to contact; the action to take and the prompt execution of that action.

Roles and Responsibilities

Commanding Officers (CO) / Heads of Establishment (HoE)

5. The CO / HoE should ensure that adequate Emergency and Disaster Plans, and major accident prevention procedures (based on the unit / establishment risk profile) are developed, exercised, evaluated, and regularly reviewed. They should include provision for Defence personnel, contractors and visitors who require special arrangements (assistance or facilities) to enable their timely evacuation without assistance from the Emergency Services and contain contingencies for any out of hours working and / or any closures of the establishment (for example, block leave). The plans should incorporate all lodger organisations on the establishment, implemented and practiced regularly as a single entity involving all stakeholders.

6. Where appropriate, resources for the provision of a staffed control centre (CC) should be made. Suitably Qualified Experienced Person(s) (SQEP) must be appointed as Incident Controller(s) (IC) having clear written terms of reference and their role and authority should be clearly identified within the Emergency and Disaster Plan documentation. Resources to enable appointment of SQEP persons in key roles are to be made available, as are any equipment needed for their role. Any shortfalls in effective implementation of these plans should be reported in accordance with Chapter 8.

7. Training should be identified, provided and evaluated to make sure that all personnel within the emergency response organisation are competent to manage all foreseeable incidents. Training and refresher training should also be provided to all personnel on the safe evacuation of buildings, vessels and the safe use of emergency equipment.

Key Personnel - Incident Controller and Nominated persons

8. The IC has the overall responsibility for directing operations, normally from the CC. During an incident the IC assumes the full authority of the CO / HoE.

9. Nominated persons such as Floor Liaison Officers (FLO), Fire Marshals etc. should provide support to the IC and act as an interface between the IC, staff and the Emergency Services attending the incident.

10. In the event of an incident, if it is safe to do so, nominated persons should report to the IC to provide technical support. Nominated persons may include:

- a. Infrastructure Manager / Maintenance Management Organisation contractor;
- b. Health and Safety Adviser;
- c. Environmental Protection Adviser;
- d. Fire Officers;
- e. Security Officers; and
- f. other specialists as required dependent on unit / establishment risks.

11. Site rules and procedures must be adhered to including as a minimum:

- a. site inductions, giving clear details on rules to be followed in the event of an emergency;
- b. ceasing work in accordance with JSP 375 Volume 3 and organisational SEMS for emergencies;
- c. security / site gate / sign in procedures; and
- d. Grab Packs.

Managers

12. Managers should ensure that all Defence personnel and visitors within their area of responsibility have received adequate training and / or been briefed in the local emergency procedures to understand what action is required of them in the event of an emergency or disaster.

13. For Defence personnel, visitors, contractors, etc. who may have a disability, medical condition etc. (temporary or permanent) which may affect their or the ability of others to respond or react to an emergency; a risk assessment (JSP 375 Volume 1, Chapter 8) should be conducted and a Personal Emergency Evacuation Plan (PEEP) produced to ensure their timely evacuation without assistance from the Emergency Services unless their assistance has been pre-agreed¹. The PEEP should take into consideration all areas where the individual concerned can be reasonably expected to visit within the establishment, vessels etc. The control measures required for a PEEP may require the manager to identify individuals and / or equipment to assist in an evacuation and appropriate additional training required (for example, use of an Evac Chair).

¹ Communities and Local Government Fire Safety Means of Escape for Disabled People

All Personnel

14. All personnel should make sure they are fully aware of the action to take in the event of an emergency, attend training as required and comply with the relevant procedure, following any additional instructions given by the IC, nominated persons or attending Emergency Services Officers. Under UK law it is an offence to fail to comply with relevant procedures or instruction and may result in staff being subject to legal and / or disciplinary action.
15. Personnel (without special emergency responsibilities) should not attempt fire-fighting or other emergency action for which they have not been trained and evacuate the building to the appropriate assembly point as soon as the alarm is heard.
16. When travelling abroad, in the UK or working in a remote location, 112 (999 works in the same way in the UK) can be dialled free of charge from any telephone or mobile phone to contact the Emergency Services (Ambulances, Fire and Rescue Service and the Police) in the European Union (EU), as well as several other countries in the world. EU Directive E112 (a location-enhanced version of 112) requires mobile phone networks to provide Emergency Services with whatever information they have about the location a mobile call was made.
17. Even if you don't know exactly where you are, using 999 / 112 on your mobile phone will allow the system to pinpoint your precise location within about 30 seconds of your call to the telecom operator and the operator automatically transmits the location information to the emergency centre so they can get the appropriate help to you as quickly as possible.
18. The Global System for Mobile Communications (GSM) standard designates 112 as an emergency number, so it will work on GSM phones even in North America where GSM systems redirect emergency calls to 911, or Australia where emergency calls are redirected to 000 (although location information may not be automatically transmitted). 999 / 112 can be dialled on most GSM phones even if the phone is locked.

Developing Plans

19. The site risk assessment (JSP 375 Volume 1, Chapter 8) is a fundamental part of the emergency and disaster planning process and should identify all activities, areas and foreseeable incidents within the unit / establishment that require measures to be taken to mitigate injury or loss. External factors both international and domestic also need to be factored into possible scenarios that might need to be managed. These may include:
 - a. fire;
 - b. medical emergency (Injury / ill health);
 - c. civil protest / civil disobedience;
 - d. entrapment (lifts, confined space etc.);
 - e. release of gas / vapour etc;
 - f. radiological;
 - g. biological;

- h. flooding;
- i. explosion;
- j. mortar attack;
- k. suspect device;
- l. vehicle borne Improvised Explosive Device;
- m. shooting; and
- n. any other emergencies.

20. The control measures required will be dictated by the risk assessment findings and more detailed actions are to be expected for the more predictable events. It is important to ensure that any guidance produced is flexible and can be adapted as an incident develops. The actions to be taken to control each credible event should follow the structure shown below:

- a. immediate response (give warning, activate alarm, etc.);
- b. initial actions (administer first aid, extinguish fire if safe to do so, contact Emergency Services, etc.);
- c. evaluate scale and nature of problem;
- d. evacuation and cordoning;
- e. use of control methods;
- f. co-operation / communication with public, press and enforcement agencies (for example, the HSE);
- g. recovery actions / business continuity; and
- h. clean up actions (longer term).

21. Emergency and Disaster Plans and procedures should immediately inform the gatehouse to enable rapid access onto site and direction to the incident for the Emergency Services. These should provide for 24-hour cover and dictate any changes between the silent hours arrangements and that required during normal working hours. In the event of an emergency on site communication is key. A tannoy systems may be used to notify those on site in conjunction with contacts listed in the major incident plans.

22. For units and establishments that include sleeping accommodation or other single occupancy rooms that may be locked, methods of rapid access (for example, the release of master / spare keys (where they exist) or forced entry) should be established and practiced for gaining emergency access. Reliance on master / spare keys alone will not be sufficient as they will be ineffectual against a door with a key left in the reverse side of the lock, a door that is bolted, or a door secured by other means.

23. For units and establishments where Major Accident Control Regulations (MACR) or Dangerous Substances and Explosive Atmospheres (DSEAR) (JSP 375 Volume 1, Chapter 9) applies, more stringent arrangements will be required and appropriate JSPs or Defence Regulations should be referred to and complied with.

24. The Emergency and Disaster Plan should be the subject of consultation with Defence personnel; this should be done through the normal consultation process (Trade Union etc) for civilians and via the Chain of Command for military personnel.

25. The Emergency and Disaster Plans should link into and meet the provisions of Integrated Contingency Planning (ICP) and the requirements of JSP 503 – MOD Business Continuity Management.

Testing Plans

26. Exercising of the Emergency and Disaster Plan should be undertaken on a regular basis (the frequency must meet the requirements of relevant JSPs and be in accordance with the level of risk but must be undertaken at least once each year). Consideration should be given to the use of external agencies to organise exercises where an independent assessment of MOD systems is required. The overall testing regime should assess procedures for silent hours as well as normal operating hours and aim to ensure that the following aspects are covered:

- a. activating the On-Site Emergency Plan;
- b. alerting Emergency Services;
- c. mobilising unit / establishment personnel;
- d. verification of adherence by personnel;
- e. activating the CC;
- f. testing the flow of information into and out of the CC;
- g. testing the internal flow of information within the CC;
- h. decision making process;
- i. command and control arrangements;
- j. verification that emergency equipment is available and operational;
- k. procedures for rapid access to locked rooms (for example, release of master keys); and
- l. public relations arrangements.

27. A post-exercise review should be conducted, documented and findings communicated to all stakeholders. If the review indicates the need to change procedures, risk assessments and / or other related documentation they should be updated and reassessed as soon as possible.

Retention of Records

28. All records including the MOD Estate / Vessel Risk Assessments, Defect Reports, etc. must be kept in accordance with JSP 375 Volume 1, Chapter 39 (Retention of Records).

Related Documents

29. The following documents should be consulted in conjunction with this chapter:

- a. JSP 375 Volume 1:
 - (1) Chapter 8 – Risk Assessment;
 - (2) Chapter 9 – Dangerous Substances and Explosive Atmospheres (DSEAR); and
 - (3) Chapter 37 – Safety at Public Events.
- b. Other MOD Publications:
 - (1) JSP 426 – Defence Fire Safety and Fire Risk Management;
 - (2) JSP 440 – The Defence Manual of Security;
 - (3) JSP 503 – MOD Business Continuity Management;
 - (4) DSA01.1 – Defence Policy for Health, Safety and Environmental Protection;
 - (5) DSA01.2 Chapter 1 – Health, Safety and Environmental Protection Requirements for Defence; and
 - (6) DSA01.2 Chapter 2 – Requirement for Safety and Environmental Management Systems in Defence.
- c. Legislation and Guidance:
 - (1) [Health and Safety at Work etc. Act](#);
 - (2) [Management of Health and Safety at Work Regulations](#);
 - (3) [Dangerous Substances and Explosive Atmospheres Regulations](#);
 - (4) [Civil Contingencies Act](#);
 - (5) [Regulatory Reform \(Fire Safety\) Order](#);
 - (6) [HSE – HSG191 – Emergency planning for major accidents \(COMAH\)](#);
 - (7) [Department for Communities and Local Government – Fire Safety - Risk Assessment – Means of Escape for Disabled People](#).

OUTBREAK MANAGEMENT

1. Defence settings are complex, with a high population density, comprised of uniformed personnel, civil servants, contractors, industry partners and dependants. This increases the probability of a military establishment becoming the focus of a local outbreak. All outbreak management plans should therefore be periodically reviewed.
2. When managing an outbreak, advice should always be checked against the latest national guidance and through the Health Protection Teams (HPTs). The Directors of Public Health have primacy for delivering the Public Health Act (Control of Diseases) 1984, contact details can be found here: [England](#), [Scotland](#), [Wales](#). Personnel in Northern Ireland should seek guidance from 38X Comd Gp. The Defence Public Health Unit is the centre of expertise and primary point of contact for all advice on public health and infectious diseases: SG-DMed-Med-DPHU-GpMailbox@mod.gov.uk.

Testing

3. Defence Advice Notice 13 gives details on how Defence personnel should access testing. Test results are not automatically communicated to the medical centre/CoC, it is therefore important that SP and other employees working on Defence establishments follow their Unit/Establishments reporting procedures regarding positive tests. This will allow prompt action to be initiated to manage risks and mitigate against outbreaks.

Outbreak Management

4. A cluster of cases is defined as *‘two or more cases associated with the same setting in a 14-day period but without a common exposure or link to each other’*. Where the investigation of the cluster identifies a *common exposure or link to other cases*, it becomes an outbreak.
5. The primacy for leading investigations, response, management, reporting, and control of COVID-19 rests with the UK Health Security Agency (HSA) and the equivalent public health organisations in the Devolved Administrations. MOD must support these efforts when they are in force to ensure a coherent response.
6. In the event that a unit, establishment or medical centre believes that it has an outbreak of COVID-19, this should be escalated to sS Public Health or Environmental Health contacts and the DPHU². There may be a need to review planned activity whilst this is managed and this should be done following the principles set out in JSP 375 Chapter 2 Annex A.

Information sharing

7. Where personal information is collected, all concerned must comply with the General Data Protection Regulations and the Caldicott principles. Fundamental to this is that the identity of any individual who has tested positive is not to be shared with contacts or other parties who do not have a need to know.

² SG-DMed-Med-DPHU-GpMailbox@mod.gov.uk