



MINISTRY OF DEFENCE

Ministry of Defence

The basic principles of working in Defence

**A guide for Service and civilian personnel,
their commanders and managers**

The basic principles of working in Defence

A guide for Service and civilian personnel, their commanders and managers

Contents

	Page Number
Introduction	2
Basic principles	4
Values and standards	5
People	7
Finance and resources	11
Contracts and commercial	15
Information	17
Communications	19
Security	21
Health and wellbeing	24
Safety	26
Sustainable development and environmental protection	28
Business Continuity	31

Introduction

As set out in the Defence Business Plan 2011-2015 and against the backdrop of the National Security Strategy and the outcome of the Strategic Defence and Security Review (SDSR), our priorities from now until 2015 are:

- To succeed in Afghanistan
- To continue to fulfill our standing commitments
- To succeed in other operations we are required to undertake
- To promote defence exports consistent with export control criteria
- To implement the Strategic Defence and Security Review
- To deliver the Defence Reform Units' review
- To deliver Defence in the most effective, efficient and sustainable way

All of us who work in Defence contribute in some way to the achievement of these priorities; this is the case whether we are Service or civilian, whatever our rank or grade, wherever we work and whatever our line of work. And in doing so, we all also have a duty to carry out our work in accordance with certain basic principles.

Who is this guide for?

This guide is for all Service and civilian staff wherever they work in Defence. It applies to all members of the Armed Forces and the MOD Civil Service; and where appropriate to others employed by the MOD, for example contractors.

The guide should be particularly helpful for new entrants as part of their induction and line managers should therefore make sure that any newcomers in their areas are aware of it and read it. It should also provide a handy "checklist" or "reminder" for the rest of us.

What is the guide for?

The guide provides a summary of the basic principles that we must follow in our day-to-day work; the general things we must remain aware of and the main general rules we must comply with over and above the particular requirements of our specialist operational or business activities. Most of it is applied common sense. It provides a quick introduction and reminder of the key principles to help people do their jobs better; and provides direction on where further detailed rules, guidance and information can be found.

What the guide is not

The guide is not a comprehensive or definitive guide to the rules and regulations that apply across Defence; nor is it a substitute for them. It is a general guide; not a statement of the particular principles and rules that apply to specialist operational or business activities.

Why is the guide necessary?

Over recent years external requirements including legal requirements with which we must comply have become more demanding. And at the same time the number of people in Defence has fallen substantially. To manage this successfully, greater responsibilities to comply with requirements have been devolved to military commanders, line managers and employees in general as part of their core responsibilities. It has therefore become increasingly important that we understand the full range of our obligations. We must be clear about what we have to do and what is expected of us in the ways we work.

The guide aims to help to clarify, simplify and communicate the basic ground rules that apply to all of us, wherever we work in Defence. It complements on-going work being carried out by those who set the rules (in particular, process owners appointed by the Defence Board) to rationalise, clarify and simplify them as far as possible for everyone, and to ensure that they are easily accessible.

What authority does the guide have?

The guide has been produced by MOD Head Office in conjunction with the relevant process owners, who are responsible for setting Defence wide policies, standards and rules. The 2nd Permanent Secretary and the Vice Chief of the Defence Staff have approved it on behalf of the Defence Board. Any separate business area guidance must be consistent with it.

How will the guide be kept up to date?

The guide will be maintained and updated, as necessary, by the Defence Business Improvement division in MOD Head Office. The current version will be published on the Defence Intranet under *How Defence Works – The Defence Framework*. The editors would value any feedback and suggestions for improvements, which should be sent to:



How to use the guide

The next section sets out the basic principles, with links¹ to subsequent sections which explain these in more depth, setting out the main things we must and mustn't do and providing direction on where we can find more detailed rules, guidance and information.

¹ Note that some of the links contained in this guide are to pages on the Defence Intranet and therefore will not work when accessing the document through the internet.

Basic principles

Wherever we work in Defence, there are certain basic principles we must follow, as set out below.

- Be aware of and act in accordance with the values and standards for Defence, set out in detail for respective Services (see **Values and standards**).
- Comply with our respective people policies and rules. In particular, ensure that Defence gets the best from its people within a working environment that is free from harassment and discrimination (see **People**).
- Ensure that any money we spend, or assets we use, are properly justified in support of Defence objectives. We must do so in a way which delivers best value for money, complies with relevant policies and rules and we must account properly for our activities. (see **Finance and resources**).
- Make sure that any contractual arrangements we enter into are made and managed by authorised commercial staff. In doing so, get best value for money, including by using corporate enabling or framework contracts wherever possible (see **Contracts and commercial**).
- Manage information properly, by storing it in the right places, making it available to those who should see it and protecting it from those who shouldn't, and keeping good operational and business records. Make the best use of information, by knowing where to find it, understanding its content and quality, adding value where needed, and communicating it clearly, quickly and securely (see **Information**).
- Help to communicate what Defence does, while complying with the rules on communicating with the media and public (see **Communications**).
- Maintain a secure working environment to protect our people, the equipment, buildings and other assets we need to do our jobs, and the sensitive information entrusted to us (see **Security**).
- Manage our health, fitness and lifestyle to ensure that we are able to meet the demands of our employment (see **Health and wellbeing**).
- Make sure that our working environment is a safe place for everyone to use and take care of our own safety and that of others who may be affected by what we do or don't do (see **Safety**).
- Minimise our use of energy (including travel), water and other natural resources. Reduce our pollution of the environment and creation of waste, and reuse and recycle more of the waste that we do produce. And consider the impact of our actions on local communities (see **Sustainable development and environmental protection**).
- Help to ensure the effective continuation of critical Defence capabilities and outputs in the event of a disruptive event, and act in accordance with plans for the longer-term recovery of Defence after disruption (see **Business continuity**).

Values and standards

We must be aware of and act in accordance with the values and standards of our respective Services.

Although each Service defines its own set of values and standards in its own particular way, they have much in common. Dependent upon our Service they require us to display values of commitment, loyalty, service, integrity, honesty, objectivity, impartiality, excellence, courage, discipline and respect; and to maintain high standards of compliance with the law, professionalism and personal behaviour. We are expected to be aware of those of our own Service and to act in accordance with them. They are set out in separate documents for each Service:

- Naval Service Core Values.
- Values and Standards of the British Army.
- Royal Air Force Ethos, Core Values and Standards.
- Civil Service Code.

What we must do

- Read and understand the values and standards of our respective Services, as set out in the documents listed above.
- Act in accordance with them.
- Report instances where we believe we are being required to act in a way that contravenes the values and standards of our Services or raises a fundamental issue of conscience or concern.

What Service commanders and line managers must do

- Make sure that those under our command or management are aware of, understand and comply with the values and standards.
- Set an example by promoting and maintaining the values and standards ourselves.

What we must not do

- Act in a way that contravenes the values and standards of our Services.
- Condone others acting in a way that contravenes the values and standards.

Where to find more information

The documents referred to above can be found via the following links:



Who to contact for more information

Any questions on the above, or requests for more information, may be directed to:

Director Naval Personnel Strategy for Royal Naval Personnel

Personal Services 2 (Army) for Army Personnel

Director Personnel and Training Strategy for RAF Personnel

DCP-CC for civilian personnel

People

We must comply with our respective people policies and rules. In particular, ensure that Defence gets the best from its people within a working environment that is free from harassment and discrimination.

Throughout Defence, Service and civilian staff work together. In addition to purely Service and purely civilian command and line management chains, Service personnel may manage civilians and civilians may manage Service personnel. Where appropriate, therefore, commanders and line managers need to be aware of, and comply with, not just the policies and rules of their own Service, but also those of their staff's Services.

We are all required to comply with employment legislation where appropriate (military personnel are exempt from some aspects), including equality and diversity legislation. Service personnel are also subject to the Armed Forces Act 2006 (covering military discipline) and Queen's Regulations (for the Royal Navy, Army and Royal Air Force).

We are also expected to play our respective parts in ensuring that Defence gets the best from its people through strong leadership, good management, training and development, teamwork and personal engagement.

The policies and rules of our respective Services are designed to ensure that we comply with the law and that we get the best from all our people. It is therefore incumbent on all of us to comply with them.

There are separate sets of policies and rules for each of our Services, as well as some that are joint. That said, there are some common key principles as set out below.

What we must do

- Be aware of the Defence priorities and objectives, as well as those of our respective units and teams, and understand how our own objectives contribute towards them.
- Be clear about our objectives and targets and the standards that are expected of us in our work, and do our best to meet them.
- Complete regular formal appraisals of our performance with our commanders or line managers.
- Regularly engage in feedback on our performance with our commanders or managers.
- Comply with the policies on equality and diversity and contribute towards a working environment free from harassment or discrimination in which we are all encouraged to reach our full potential and are treated on our merits.
- Take appropriate action against bullying, harassment, unlawful discrimination, prejudice, and negative attitudes displayed by others.
- Be aware of our remuneration packages and the claims processes for allowances, including our individual responsibilities to ensure we only submit claims that are properly authorised and within our entitlements.

- Keep our records on the Service joint personnel administration system or the civilian human resource management system accurate and up to date.
- Carry out our work with political impartiality at all times.
- Ensure that Service discipline is maintained at all times.

We should also

- Be prepared to learn and develop and be flexible in response to changing requirements.
- Seek to improve our contribution to overall performance by becoming more involved and engaged in the work of our units and teams, and by offering our views on how performance may be improved.
- Welcome, respect and value the contributions of others to the overall performance of our units and teams.
- Be aware of the procedures for expressing grievances or making complaints and the support available to us.

What Service commanders and line managers must do

- Ensure that those under our command or management are aware of the Defence priorities and objectives, as well as those of our respective units and teams, and understand how their own objectives contribute towards them.
- Set clear objectives, targets and standards for those under our command or management, and challenge and support individuals and teams to meet them.
- Undertake regular formal appraisals of performance.
- Regularly engage in feedback on performance, including an active interchange of honest views.
- Promote learning and development of individuals and teams and flexibility in response to changing requirements.
- Seek to improve overall performance by involving and engaging members of our teams in decisions that affect them, and by inviting their views on how performance may be improved.
- Provide effective leadership through the demonstration of professional competence, fairness and openness, effective authority and firm but fair discipline.
- Where appropriate, recruit and promote on merit via the relevant Service procedures.
- Reward and recognise individuals according to their contribution to operational and business objectives regularly and specifically during regular appraisals.
- Ensure compliance within our teams with the policies on equality and diversity and a working environment free from harassment or discrimination in which all are encouraged to reach their full potential and are treated on their merits.
- Take appropriate action against bullying, harassment, unlawful discrimination, prejudice, and negative attitudes displayed by members of our teams.

- Ensure that our teams are aware of the procedures for expressing grievances or making complaints and the support available to them.
- Ensure that our teams are aware of their remuneration packages and the claims processes for allowances, including their individual responsibilities to ensure they only submit claims that are properly authorised and within their entitlements.
- Ensure that team members keep their records on the Service joint personnel administration system or the civilian human resource management system accurate and up to date; and provide the required command or management inputs to these systems.
- Where managing civilian staff, ensure we consult with our local human resource business partner and the Trades Unions where appropriate on proposals which affect our employees.
- Provide reasonable adjustments to the working environment for team members with disabilities.
- Ensure that Service discipline is maintained at all times

What we must not do

- Take part in activities that might conflict with the interests of, or discredit, Defence.
- Make use of our official position to further our private interests or those of others, or lay ourselves open to suspicion of dishonesty.
- Put ourselves in a position where our official duties and private interests conflict with each other.
- Engage in behaviour that risks degrading our professional ability or damaging the trust and respect that must exist between individuals who depend on each other.
- Participate in industrial action or any form of political activity organised by a formally constituted independent professional organisation (Trade Union or federation) (Armed Forces personnel only).

Mandatory Training

- Equality and Diversity – (Module VR008N) to be undertaken every three years for civilian staff.
- Equality and Diversity training will vary for Service personnel depending upon their Service.

Where to find more information

Further advice and information can be obtained from local or unit personnel offices for Service personnel. Information can also be found via the following links:



*for civilian personnel matters and human resource management system.

Who to contact for more information

Any questions on the above, or requests for more information, may be directed to:

The relevant local unit Personnel/Admin Officer for Service personnel matters and the People Pay and Pensions Agency for civilian personnel matters.

Finance and resources

We must ensure that any money we spend, or assets we use, are properly justified in support of Defence objectives. We must do so in a way which delivers best value for money, complies with relevant policies and rules and account properly for our activities.

Good financial and resource management is the responsibility of each and every one of us. This is because nearly everything that we do has a financial implication. The requirement for good financial housekeeping relates to expenditure in single or tens or hundreds of pounds, as well as to expenditure on large equipment programmes which may be measured in millions or billions of pounds.

All expenditure must contribute towards Defence and comply with the relevant rules

The Defence budget is allocated to us by Parliament for delivering Defence objectives. Like all public services, Defence activities are funded by taxpayers, which includes us. We must spend money from the Defence budget only on those purposes for which it is given, and in line with relevant legislation and other external rules (such as the Treasury's 'Managing Public Money'). The same applies to the way in which we use our other assets, including people, equipment (whether in the field or office) and estate. Using money and assets for their intended purpose, and in line with legislation and external rules, is what is meant by acting with 'propriety and regularity'. The financial and resource management policies and rules set out by MOD and local financial authorities are designed to ensure that we comply with legislative and other external requirements, as well as obtaining best value for our resources. It is therefore incumbent on all of us to comply with them.

We should remember that any money spent, or asset used, not in support of meeting Defence objectives means that less is available to support the sailors, soldiers, airmen and civilians working on front-line activities. If we are unable to match the activity which we are carrying out to a wider Defence objective, we must review the activity and seek further guidance from our budget manager. This is because we may be spending money or using assets inappropriately.

Authority to spend money

The authority to spend Defence money is delegated from the MOD Permanent Secretary to top level budget holders and then down the budgetary chain to named individuals. These delegations are subject to specific limitations and requirements, which are set out in individual letters of delegation. Only those in receipt of such delegations are authorised to spend Defence

money. Budget managers throughout the budgetary chain provide advice and support to those with delegated authority to ensure that they comply with the financial policies and rules and the terms of their delegations.

We must deliver value for money for every pound we spend

Value for money is about maximising the benefit we obtain from the resources available to us – both money and assets. Ministers, senior Service officers and civilian officials are regularly called by Parliament, the public and the press, to justify the way in which we use our resources. To ensure that we achieve value for money in everything we do means we must consider a range of options as to how we might best meet our objectives. This usually means seeking the advice of our budget managers about how to make properly informed decisions. Value for money may not always mean the cheapest option; for example, it may be more cost effective to buy a more reliable service or a better quality asset with lower maintenance costs and a longer operating life.

All expenditure must be properly accounted for and auditable

Every year each top level budget holder, including the Chiefs of Staff, must produce a set of financial accounts which explain how they have spent each taxpayers' pound, and how each of our assets are used throughout the period. These are consolidated into a Defence-wide set of accounts. The MOD's Permanent Secretary, as the Accounting Officer, submits the accounts to the Treasury and will go to Parliament to answer questions about them. We must, therefore, ensure that adequate evidence is maintained for audit purposes so that we can prove that the accounts are accurate and that we are spending public money only on meeting Defence objectives.

If we are seen by Parliament, the public and the press to be using Defence money and assets for activities not in support of Defence objectives, or we are unable to account for the money we spend and the way we use our assets, then we are at greater risk of doing relatively less well when the Treasury makes decisions about how to allocate money across the public sector.

What we must do

- Comply with Departmental and local financial and resource management policies and rules.
- Be able to explain how any activities we undertake relate to our agreed objectives.
- Have our budget manager's agreement to spend money, or to use other resources, including their confirmation that the expenditure is affordable, meets team and Defence objectives, and is in line with the relevant rules.
- Assess a number of options, including the 'do nothing' option, about how best to achieve the desired outcome when we are proposing to spend money or use resources.

- Go about our daily work in line with the standards expected of all public servants - both Service and civilian - responsible for using and managing public money and assets (honesty, impartiality, openness, accountability, accuracy, fairness, integrity, transparency, objectivity and reliability).
- Ensure that an accurate record is made of expenditure (and income) for which we are responsible, and any asset that we use, so that the annual set of accounts may be produced. Our budget manager can advise us how to do this.
- Copy any submissions to Ministers which have financial implications (and most do), to our budget staff, and to the Director General Finance or his London-based staff.
- Ensure that we spend money within the limits of the financial delegation personally issued to us.
- Ask ourselves what the presentational implications are for the way in which we plan to spend taxpayers' money and use taxpayers' assets.
- Be prepared to explain the way in which we have spent money, or used assets, to our commander or manager .
- Seek advice from our local finance team if we are in any doubt about whether what we are doing, or what we have been asked to do, does not comply with the relevant external and internal rules relating to finance.
- Before embarking on any new course of action, or on the development of any new policy, we should consult our finance teams so that potential resource implications may be considered from the outset.

What we must not do

The Department has a **zero tolerance to fraud**. It is also the case that a failure to observe the key principles of propriety and regularity constitutes an **abuse of financial authority**. Any such abuse can lead to disciplinary action being taken against the individual, or individuals, even where there is no personal gain. In addition to considering those general principles at all times we must not:

- Break the law.
- Bend or break the external or internal financial rules in an attempt to achieve advantage or improved results.
- Deceive or knowingly mislead decision makers about the cost, or value for money, of a proposal to spend money or use assets.
- Allow a conflict of interest to affect, or appear to affect, our judgement relating to any decision about spending money or using assets.
- Spend money, or use assets, in a way which does not support Defence objectives. This includes making donations to charities and welfare funds, no matter how good the cause is.
- Commit to, or approve, spending money which is not affordable within the agreed budget.
- Use, or be party to the use of, public money for private benefit, whether our own benefit or that of others.

Mandatory Training

The Financial Skills Certificate Foundation for roles in the Finance function.

Where to find more information

Information on financial and resource management can be found on the Finance hub on the Defence Intranet and from our local finance and budget teams:



Who to contact for more information

Any questions on the above, or requests for more information, may be directed to:

DFM-FMPD-Pol Com1

Contracts and commercial

We must make sure that any contractual arrangements we enter into are made and managed by authorised commercial staff. In doing so, get best value for money, including by using corporate enabling or framework contracts wherever possible.

MOD commercial policy and procedures are set out in the Commercial Toolkit within the Acquisition Operating Framework. They are derived from contractual and European law which is detailed and complex. It is essential, therefore, that officers holding commercial delegations are involved from the earliest stages and throughout negotiations over the procurement of goods, services and works.

While many budget holders have the authority to enter into contractual commitments from the resources available within their budgets, MOD policy is that only individuals holding a commercial delegation may actually let a contract. We all must take care not to contractually commit the Department without the appropriate authority to do so. If we do make any commitments on behalf of the MOD (either verbally or in writing) without being correctly authorised, we may be held personally liable for the full value of the commitments and may face serious disciplinary proceedings.

What we must do

- Avoid unintentional contracts both verbal and written.
- Ensure that any contracts that we are responsible for provide the best value for money.
- Use corporate enabling/framework contracts wherever possible – these contracts have been established for a variety of goods and services and provide pre-competed value and a rapid and easy route to supply.
- Preface all discussions about potential requirements with contractors, including amendments of existing contracts, by a statement that they are on a 'without commitment' basis.

We should also

- Ensure that commercial staffs are involved and their advice sought at the earliest stage of any purchase, of whatever size or complexity.
- Consider whether our requirement is or could be part of a bigger requirement and what opportunities exist to co-ordinate with others to get a better deal – once again, take advice from commercial officers.
- Ensure that the true through-life cost of a purchase is considered – not just the initial purchase price.

- Ensure we maintain a clear rationale and audit trail for the commercial arrangements we enter into.

What we must not do

- Contractually commit the Department without authority from someone with the appropriate commercial delegations.

Where to find more information

Information on commercial management can be found on the Acquisition Operating Framework and from our local commercial officers:



Who to contact for more information

Any questions on the above, or requests for more information, may be directed to:

DGDC-CS

Information

We must manage information properly, by storing it in the right places, making it available to those who should see it and protecting it from those who shouldn't, and keeping good operational and business records. We must make best use of information, by knowing where to find it, understanding its content and quality, adding value where needed, and communicating it clearly, quickly and securely.

Information is the lifeblood of Defence, and our success can depend on how well we exploit information. Managing information well is a prerequisite to exploiting it effectively. MOD policy on information management is in Joint Service Publication 747, where there is also a series of information management protocols providing advice on how to manage information effectively.

What we must do

- Use our shared areas for all significant information, including the MOD records management system for anything that needs to be preserved unaltered – don't squirrel information away in e-mail accounts or personal storage.
- Make sure information is available to those who should have access to it, but protected from those who shouldn't – we should share information responsibly and sensibly through correct use of folder and library permissions.
- Label information properly, using the MOD standards, and store it in the appropriate containers (e.g. the right folder or document library).
- Understand how to use our systems, so that we can store, communicate and retrieve information quickly and accurately.
- Be aware of the four most important bits of information legislation, and check the detail when we need to:
 - Official Secrets Act (we must not disclose information improperly);
 - Public Records Act (we must keep a good record of our business);
 - Data Protection Act (we must look after personal information properly); and
 - Freedom of Information Act (we must respond to written requests for access to information).
- Know the rules about carrying and encrypting Defence information on portable devices such as laptops, memory sticks, and DVDs or CDs, or transmitting it over the internet – and minimise the risk of loss.
- Whenever we are using MOD IT, follow the Acceptable Use Policy (Joint Service Publications 740), and the Security Operating Procedures for the system concerned.
- Know who in our unit has specialist responsibility for information, in particular the Senior Information Officer, Information Manager, and Information Support Officer.
- Show personal responsibility whenever handling information, and demand the same standards from staff and colleagues.

- Know where to find advice on good information management practice, in particular the information management protocols (Joint Service Publication 747) and guidance from our top level budget.

We should also

- Help other people to find us when they need to – keep our Calendar open and up to date, use our Out of Office indicator and voicemail message when we are away, and ensure our e Directory entry is valid.
- Communicate wisely – information is of most value when it is made available to the right person at the right time, in the right format, and to the right level of quality – don't inundate colleagues with unnecessary copies.
- Write with accuracy, brevity, and clarity – plain English is always best.
- Complete the Defence Information Management Passport. Ensure that we attain the Defence Information Passport in order to show that we understand and can apply the basic principles of good information management required by Defence and encourage others to do the same.

Mandatory Training

Protecting Information Level 1 annually (Level 0 for Service personnel in Land Forces).

Where to find more information



Who to contact for more information

Any questions on the above, or requests for more information, may be directed to:

CIO-COS

Communications

We must help to communicate what Defence does, while complying with the rules on communicating with the media and public.

Developing a greater understanding of what we do and what we have achieved amongst our external stakeholders – Parliament, public, press (at home and abroad), allies and other Government departments – and our own people is extremely important. It helps maintain a strong reputation for Defence. In turn, that sustains public support for current operations, the Armed Forces and the Defence budget, and underpins recruitment and retention of the people we need to deliver success.

The Defence Communications Strategy sets out what our communications priorities should be and describes the responsibilities of everyone in Defence – military and civilian, whether professional communicators or not – for helping to explain what we are about.

What we must do

- Obtain the necessary authorisation before contacting the media or to write or speak in public on Defence matters. How to do this is set out in Defence Instructions and Notices 2008DIN03-020.
- When dealing with a policy change or other development that needs to be communicated, or has the potential to impact on our people or draw criticism from the press, we should:
 - make sure we have engaged Defence Media and Communications at an early stage; and
 - ensure that the presentational issues are fully covered in any submissions to Ministers.
- Communicate with our colleagues and staff, and ensure they receive (or have access to) the information they need, when they need it, and there are suitable feedback mechanisms in place. Make use of internal communication products (e.g. Internal Briefing Notes and Digests, Intranet news and announcements) to keep them in touch with what is happening. An internal communications strategy is published on the intranet.

We should also

- Consider how we can portray our work in an interesting and accessible way so that what the Armed Forces and MOD do and achieve are understood better.
- Look for opportunities to explain what Defence is about to both internal and external audiences. One way to do this is through the use of social media (see Defence Instructions and Notices 2009DIN03-020 for further guidance).
- Use our internal channels (internal briefing notes, the intranet, in-house magazines and Service journals) in addition to local channels and products to reach our target audience and complement wider Defence communications.

- Engage with our stakeholders via meetings, exhibitions, events and roadshows, as well as considering how to engage audiences by putting in place feedback mechanisms and acting on them.
- Utilise the skills, experience and contacts of the dedicated communications and media experts embedded throughout Defence who can provide advice and support on dealing with the media and communicating on Defence issues. Their contact details can be found in Defence Instructions and Notices 2008DIN03-020.

Where to find more information

Further information and advice on media and communications and access to the above Defence Instructions and Notices can be found in the link below:



Who to contact for more information

Any questions on the above, or requests for more information, may be directed to:



Security

We must maintain a secure working environment to protect our people, the equipment, buildings and other assets we need to do our jobs, and the sensitive information entrusted to us.

Every organisation needs to protect its people, assets and information from attack or compromise. This is a principle of both business and military operations. The basics of security in Defence are easy to understand, and are set out below.

Protecting ourselves and other people

Historically, there has been a risk of terrorist attack against Defence personnel, particularly those in the Services. This risk has changed, is not as high but could fluctuate. For now the best advice is simply to keep an eye open for anything that looks suspicious in or around a Defence site (unattended luggage or containers, people on-site without identity passes, people acting suspiciously in or around the site, etc). We should report anything suspicious to our local security officer or line manager.

Protecting our assets

The same basic principles apply. Look out for and report people acting suspiciously, evidence of theft, vandalism or damage, and do whatever we can to ensure valuable and potentially dangerous items are kept securely when not in use.

Protecting our information

For a number of reasons, this is currently the security area of greatest risk. It is comparatively easy, through everyday social behaviour, inadvertently to reveal Defence-related information to others. There are terrorist groups and foreign intelligence organisations that are actively trying to acquire as much information as they can about Defence, or about key people who work in Defence, even if this comes in scraps from a range of different sources. And internal information which becomes public can also be reported in uninformed and unbalanced ways by the media, thus unfairly damaging the reputation of Defence.

It is important not to over-state these risks, however. We are generally free to talk about ourselves and our work, both in conversation and through on-line social media, provided we follow basic principles about protecting sensitive kinds of information.

What we must do

- Keep an eye open for anything that looks suspicious in or around a Defence site (unattended luggage or containers, people on-site without identity passes, people acting suspiciously in or around the site, etc).

- Report anything suspicious to our local security officer, commander or manager.
- Look out for and report people acting suspiciously, evidence of theft, vandalism or damage.
- Switch mobile phones off (and if required hand them in) when asked to do so – they are more vulnerable than many might think.
- Protect passes, identity cards, passwords, personal identity numbers and combination numbers.
- Inform our unit or organisation of any changes in our personal circumstances (e.g. marriage); including if we are arrested for any reason. Otherwise we might find ourselves wrongly classed as a security risk.
- Be completely open with the Defence vetting process, as it affects us. Vetting is one of the main ways we insure against our information being compromised from within, and while the process can sometimes seem rather intrusive at a personal level, it is important that it operates effectively. Being open in responding to vetting questions will help show that we are trustworthy and honest; failure to do so, on the other hand, is likely to lead to serious questions about our fitness to hold a security clearance.

We should also

- Do whatever we can to ensure valuable and potentially dangerous items are kept securely when not in use.

What we must not do

- Discuss any details of military equipment, training, tactics, techniques, intelligence or operations (this could put lives at risk on the battlefield).
- Discuss plans, policy or doctrine (again this could endanger lives or damage the UK's international relations).
- Reveal personal information about other people (names, addresses, phone numbers, photographs), and especially don't reveal sensitive personal data such as bank, medical, or vetting details. This information is protected by law.
- Give details that are commercially sensitive in Defence dealings with its suppliers.
- Reveal information which could be misleadingly sensationalised by the media.
- Disclose details about ourselves, or others, which could alert and help hostile organisations to apply blackmail or other forms of pressure.
- Discuss the above kinds of information on an open landline or mobile phone – this type of communication is easily, and routinely, monitored.
- Remove documents or items which have protective markings unless we really have to. And when we do, we must follow the correct rules for getting authorisation and keeping them secure (e.g. don't read them in public places where we can be overlooked).
- Remove laptops or other portable IT media unless they are certified as being fully encrypted (it's our job to check). When removed, keep them secure, protect login details and store secure keys separately from the laptops they unlock.

Where to find more information

Further information can be found on the Defence Security homepage.



Who to contact for more information

Any questions on the above, or requests for more information, may be directed to:

DBR-DefSy-SySec 2.

Health and wellbeing

We must manage our health, fitness and lifestyle to ensure that we are able to meet the demands of our employment.

The physical and psychological demands of working in Defence vary widely; from those experienced in the operational environment to those in back office functions. It is important to maintain our health, fitness and lifestyle as appropriate to ensure that we are able to meet the demands placed upon us.

What we need to do in this respect will depend on our particular circumstances; but there are nonetheless some common basic principles, as well as some which apply broadly to either military or civilian personnel.

What we must do

- Take responsibility for our own health, fitness and lifestyle.
- After contracting or coming into contact with someone with an infectious illness, inform our commander or line manager immediately, so that precautionary steps can be taken to protect other members of staff.
- Ensure our details on the Service joint personnel administration system or civilian human resource management system are kept up to date with personal and contact information.

What Service commanders and line managers must do

- Support our team members in their efforts to assume responsibility for their own health, fitness and lifestyle.
- Inform our civilian team members when we intend to ask for occupational health advice, explain the reason for the referral and what can be expected.

As Service personnel, we must

- Ensure that we are able to undertake our Service fitness test at any time (unless exempt).
- Attend any medical appointment booked for us to avoid waste of valuable resources, or if unable to attend inform our medical centre/hospital immediately so that the appointment can be re-allocated.
- If we receive emergency healthcare from a civilian provider (NHS or private) during silent hours or periods of leave, give the details of our unit medical centre to the NHS or private provider.
- Inform our unit immediately if a GP provides us with a medical certificate that excuses us from work.

- Expect health surveillance in certain locations and occupations.
- Expect to receive periodic health screening and be provided with access to healthcare that is at least comparable to that provided by the NHS, excepting where unattainable due to the operational environment.

As civilians, we must

- Maintain a safe and healthy working environment and achieve a good work life balance to keep ourselves fit and healthy to attend work.
- Ensure that our manager (or other appropriate individual) is informed in line with local procedures if we are unwell and unable to attend work, advising how long we think we may be away from work.
- Ensure that any period of sick absence is recorded on the human resource management system, where we have an account, either by our manager or ourselves.
- Follow the sick certification process; any absence that exceeds seven calendar days must be supported with a medical certificate.
- If suffering an accident at work contact our relevant Incident Notification Cell.
- Contact the Occupational Welfare Service helpline for advice and support if we have a work-related or personal problem that is affecting our performance or attendance where our manager cannot help or where it would be inappropriate to involve our manager.
- If referred to Occupational Health, cooperate with the provider. It is in our interests to take part in a telephone consultation or attend any appointments with the provider.

Where to find more information

Additional advice for Service personnel



Additional advice for civilian employees (Defence Intranet):



Who to contact for more information

Any questions on the above, or requests for more information, may be directed to:

SG ACDS-ACDS Health COS

Safety

We must make sure that our working environment is a safe place for everyone to use and take care of our own safety and that of others who may be affected by what we do or don't do.

We must comply with the Health and Safety at Work Act. Any death or injury at work is regrettable, but the consequences for both the victim and the victim's family can often be severe, life changing and heart-rending. For the Department, accidents and injuries can also be costly, can affect delivery of objectives, and can result in legal action and adverse media coverage. The Defence Board has made it clear that it expects all of us to play our part in reducing the number of work-related accidents.

What we must do

- Take care of our own safety and that of people who may be affected by what we do (or do not do).
- Co-operate with others, including our commanders, managers, colleagues and contractors, to ensure all activities are undertaken in a safe way, and that rules and procedures are followed.
- Undertake fire and safety training as specified in unit and local arrangements.
- Tell someone (for example, our commander, manager or safety representative) if we think the work or inadequate precautions are putting anyone's safety at serious risk.
- Report accidents and incidents, including near misses, to our commander or manager.
- Read the ***Secretary of State's Policy Statement on Safety, Health, Environmental Protection and Sustainable Development*** to help understand safety in Defence.
- Ensure we fully understand emergency procedures in our place of work, including any requirements for helping persons who may have physical difficulty in leaving the building in an emergency, which may require production of Personal Emergency Evacuation Plans.

What Service commanders and line managers must do

- Carry out the appropriate risk assessments on activities for which we are responsible.
- Ensure that safety measures identified by risk assessments are implemented.
- Use the services of competent persons, such as local safety advisers, to help carry out risk assessments and implement safety measures.
- Make sure any accidents or near misses to members of our teams are reported to the relevant unit incident notification cell or local safety adviser and ensure a proportionate investigation is undertaken.

- Make sure members of our teams are provided with clear information, training and supervision to undertake their tasks safely.

What we must not do

- Ignore safety rules.
- Interfere with, or misuse, anything provided for our health, safety or welfare.

Where to find more information

Further advice and information can be obtained from our local health and safety representatives or from:



Who to contact for more information

Any questions on the above, or requests for more information, may be directed to:

DBR-SSDC-Safety AH.

Sustainable development and environmental protection

We must minimise our use of energy (including travel), water and other natural resources. We must reduce our pollution of the environment and creation of waste, and reuse and recycle more of the waste that we do produce. And we must consider the impact of our actions on local communities.

What do we mean by sustainable development?

At the global and national level **sustainable development** (SD) is about finding a balance between economic growth, environmental stewardship and social progress which is sustainable for the long-term.

In the MOD, **environmental protection** (EP) is the part of SD covered by environmental legislation.

SD and Defence

The delivery of Defence capability will be increasingly threatened by interlinked environmental and social challenges such as climate change, natural resource depletion, water scarcity and population growth.

To ensure the continued delivery of effective and efficient capability, Defence must improve its resilience by adapting to these threats, and by playing its part in mitigating them. This is encapsulated with the following **Defence SD principles**:

Principle 1: Defence must be resilient to current and future environmental, social and economic threats (adaptation).

Principle 2: Defence must minimise the negative, and realise the positive impacts, that Defence activities have on the environment, people and the economy in the UK and overseas (mitigation).

Far from being a burden, adaptation and mitigation will have significant benefits for Defence. For example:

- Less reliance on fossil fuel in theatre presents us with a significant opportunity to reduce the amount of fuel that has to be transported to the front line; a costly, risky and logistically resource intensive activity;
- Considering issues such as the effects of climate change and resource depletion/availability in our equipment, infrastructure and policy planning, and adjusting and adapting our behaviour now, will cost less than trying to adapt in the future;
- Using less resources, energy, fuel and water and producing less waste will save money across Defence;
- Developing positive relationships with local communities in the UK and overseas can increase support for Defence, generating favourable conditions in which to conduct our business, as well contribute to the success of military operations.

The new MOD Business Plan reflects the importance of SD to Defence by naming it as **one of seven Defence priorities**:

*To deliver Defence in the most effective, efficient and **sustainable** way by meeting benchmarking, efficiency and Government sustainable development targets, building on the Defence Reform Unit's review*

What we must do

- Minimise our use of energy by, for example:
 - reducing travel, particularly by air or car;
 - cycling, walking or using public transport to travel to work, where possible;
 - turning off monitors (and shutting down base units), unplugging mobile phone chargers and other equipment when not in use;
 - reporting areas that are too hot, cold or draughty; and
 - where possible, turning down heating/air conditioning and turning off unnecessary lighting.
- Minimise our use of water and other natural resources by, for example:
 - turning off taps and reporting leaks;
 - using recycled paper, printing on both sides of the paper or not printing at all;
 - using reusable cups, rather than disposal ones; and
 - only buying what we need.
- Minimise production of waste and recycle or reuse more of the waste we do produce by using existing recycling facilities or asking for facilities if they don't already exist.
- Minimise air, water and land pollution by, for example:
 - reporting spills of oil or paint immediately; and
 - being aware of Health & Safety and Environmental Protection procedures in our area.

- Consider the impact of our actions on local communities in the UK and overseas and help to promote Defence by, for example:
 - always considering the reputation of our unit when socialising in communities located near military bases;
 - being a good neighbour by helping and supporting the community; and
 - taking part in volunteering schemes, e.g. becoming a school governor.

What Service commanders and line managers must do

- Ensure that our activities comply with legislation and assess all of our decisions against sustainable development principles (i.e. show how we have balanced the social, environmental and financial impact of our decisions).
- Lead by example and articulate to our teams how and why we are integrating sustainable development principles into our decision making.
- Ensure our staff are aware of the importance of sustainable development and what they can contribute.
- Take action to 'green' our office space (see individual actions above).

Where to find more information:

Further information can be found at:



Who to contact for more information

Any questions on the above, or requests for more information, may be directed to:

DBR-SSDC-SDEnquiries@mod.uk

Business continuity

We must help to ensure the safe and secure continuation of critical Defence capabilities and outputs in the event of a disruptive event, and act in accordance with plans for the longer-term recovery of Defence after disruption.

What do we mean by a resilient organisation?

An organisation that is able to resist being affected by an incident, understands the threats, hazards and risks to its operation, and puts in place measures that minimise the likelihood and impact of disruptions on its people, processes and resources (including reputation).

What do we mean by business continuity?

Every organisation can be subject to disruptions such as technology failure, fire, flooding, utility disruption and terrorism. Successful business continuity management identifies what needs to be done before an incident occurs to protect people, premises, technology, information, supply chains, stakeholders and reputation. This enables organisations to develop appropriate responses (strategies and plans) to manage the consequences of disruption, mitigate the impact on critical activities and outputs, and recover business back to normal levels of operation as soon as possible afterwards.

Why is business continuity management important to Defence?

Defence plays a key role in defending the UK and its interests and in strengthening international peace and stability. Defence has a unique set of responsibilities within Government that must continue to be met regardless of what may occur.

What we must do

- Know where to go in the event of an incident. Information will be on communal notice boards about evacuation and assembly points. Our unit's business continuity plan should describe the longer-term arrangements that apply if the disruption is more severe or likely to extend beyond a few hours, such as moving to an alternative building or site.
- Know what to do if we are sent home after an incident. We will be given instructions at the time, but we should also know what our unit's business continuity plan requires. The plan will tell us who to contact. If it is a major incident, information may also be given on radio or TV. We should also check for information at **www.mod.uk**.

- Be aware of how quickly the work we do must be resumed following a disruptive event (its criticality status). If we don't know the criticality status of our work, we should consult our chain of command or management, refer to our unit's business continuity plan or ask our unit's business continuity planner as soon as possible. Remember that higher rank does not always mean higher criticality.
- Know what to do to assist the recovery of the organisation back to normal operations. Some individuals may have specific roles and responsibilities for business recovery (for instance as members of business recovery teams), and these details should be set out in our unit's business continuity plan. Individuals doing work which is less time critical may be asked to help out with other more time critical activities or outputs.

What Service commanders and line managers must do

- Ensure that our teams are aware of the unit business continuity plans.
- Provide any support required by business unit and site planners, and actively encourage and raise awareness of business continuity.
- Consider resilience and business continuity issues alongside other more familiar planning and management activities.

Mandatory Training

We should all undertake the Business Continuity awareness e-learning training on the Defence Learning Portal/Defence E-Learning Centre. How often we should do this depends upon the TLB within which we work.

Where to find more information

General information for everyone in Defence can be found at:



Who to contact for more information

Any questions on the above, or requests for more information, may be directed to:

DBR-SSDC-BC Group (email)

or 9621 82729 / 88328 / 70215

