Privacy Statement – Defence Force Recruiting

Purpose

The document details the policies that will be applied by the Department of Defence and its contracted service provider Manpower Services (Australia) Pty Ltd (together referred to as Defence Force Recruiting (DFR)) to ensure that the Australian Defence Force (ADF) recruiting process is conducted in compliance with the *Privacy Act 1988* and Australian Privacy Principles (APPs) in the management of personal and sensitive information.

The *Privacy Amendment (Enhancing Privacy Protection) Act 2012* amended the *Privacy Act 1988* with effect from 12 March 2014, and replaced the Information Privacy Principles (IPPs) and National Privacy Principles (NPPs) with the Australian Privacy Principles. To view the *Privacy Act 1988*, and the APPs, refer to the ComLaw website: www.comlaw.gov.au.

References to Corresponding Documents:

ADFRI011	Storage, Transfer and Disposal of Recruiting Documentation
ADFRI049	Legal Requests for Information
ADFRI050	Release of Documents to Candidates
ADFRI021	National Police Checking Service
DFR-RECPRO168	Identification Verification Procedure
DFR-RECFOR081	National Police Checking Service (NPCS) Application/Consent Form

Australian Government – Office of the Australian Information Commissioner (Website)

Australian Government – APP Guidelines (Website)

Australian Government – ComLaw (Website)

Australian Government – Department of Defence (Website)

Manpower Services Australia Privacy Policy (Website)

Responsibility for Implementation:

All DFR staff

Table of Contents

Privacy Statement – Defence Force Recruiting 1
Privacy Act 1988 4
Australian Privacy Principles (APPs) 4
DFR's Privacy Statement 5
Enquiries and Complaints 5
Policy 1 - Open and Transparent Management of Personal Information (APP1) 6
Availability of Privacy Statement 6
Policy 2 - Anonymity and Pseudonymity (APP2) 6
Policy 3 - Collection of Solicited Personal Information (APP3) 7
Collection of Personal Information 7
Collection of Sensitive Information 7
General Types of Information Collected 8
Policy 4 - Dealing with Unsolicited Personal Information (APP4) 9
Policy 5 - Notification of the Collection of Personal Information (APP5) 10
Collection of personal information from someone other than the relevant individual 10
Consequences for the individual if personal information is not collected by DFR 11
Policy 6 - Use or Disclosure of Personal Information (APP6) 11
Policy 7 – Direct Marketing (APP7) 12
Policy 8 - Cross Border Disclosure of Personal Information (APP8) 13
Policy 9 - Adoption, Use or Disclosure of Government related Identifiers (APP9) 13
Policy 10 - Quality of Personal Information (APP10) 13
Policy 11 - Security of Personal Information (APP11) 13
Identification Verification Procedures 14
Secure Destruction and De-Identification 14
Defence Jobs website and Online Services 14

Policy 12 - Access to Personal Information (APP12) 14

Access Charges 15

Refusal to Give Access 15

Policy 13 - Correction of Personal Information (APP13) 15

Correction Charges 15

Refusal to Correct Information 15

Policy 14 - Medical Information 16

Policy 15 - Psychological Information 16

Policy 16 - Digital Media and Electronic Tracking 16

Internet Service Provider (ISP) 16

Cookies 17

Social Media and Third Party websites 17

Opting out 17

Privacy Act 1988

The *Privacy Act 1988* includes a set of privacy principles – also known as Australian Privacy Principles (APPs) – which regulates the handling of personal information by both Australian Government agencies and organisations.

In accordance with section 6 of the *Privacy Act 1988* "personal Information" is defined as "information or an opinion about an identified individual, or an individual who is reasonably identifiable:

(a) whether the information or opinion is true or not; and

(b) whether the information or opinion is recorded in a material form or not".

Australian Privacy Principles (APPs)

The 13 APPs are:

- APP1 – Open and Transparent Management of Personal Information
- APP2 – Anonymity and Pseudonymity
- APP3 – Collection of Solicited Personal Information
- APP4 – Dealing with Unsolicited Personal Information
- APP5 – Notification of the Collection of Personal Information
- APP6 – Use or Disclosure of Personal Information
- APP7 – Direct Marketing
- APP8 – Cross-Border Disclosure of Personal Information
- APP9 – Adoption, Use or Disclosure of Government related Identifiers
- APP10 – Quality of Personal Information
- APP11 – Security of Personal Information
- APP12 – Access to Personal Information
- APP13 – Correction of Personal Information

To review the complete APPs and the APP Guidelines published by the Office of the Australian Information Commissioner (OAIC), refer to the OAIC's website; www.oaic.gov.au.

DFR's Privacy Statement

DFR provides managed recruiting services for the Australian Defence Force (ADF), including (but not limited to) marketing, promotion and recruiting selection processes. DFR collects, holds, uses and discloses personal information for the purposes of;

- marketing and promoting ADF jobs, careers, brands and activities;
- informing individuals of ADF jobs, careers and lifestyle;
- receiving and managing enquiries and applications related to the managed recruiting services;
- assessing an individual's eligibility and suitability for service with the ADF;
- facilitating job offers, transfers and the enlistment or appointment of an individual to the ADF and Single Services; and
- research into improving the managed recruiting services.

DFR's privacy statement is aligned with the APPs. These policies are detailed within each of the sub-headings within this statement.

This statement is limited to the activities of DFR in relation to provision of managed recruiting services for the ADF. It does not apply to other activities of the Department of Defence or of Manpower Services (Australia) Pty Ltd which do not relate to provision of managed recruiting services for the ADF. These are governed by the general APP privacy policies which apply separately to each of those entities which are available at www.defence.gov.au and www.manpower.com.au.

Enquiries and Complaints

All enquiries and complaints related to DFR's compliance with, or breach of, the APPs should be directed to defence.privacy@defence.gov.au (email), via 13 19 01 (phone) or via Site Management at the individual's nearest Defence Force Recruiting Centre (in writing or in person).

The location of Defence Force Recruiting Centres can be found on the Defence Jobs website: www.defencejobs.gov.au/recruitmentCentre/contactUs/#

We will take reasonable steps to investigate any complaint, and to notify you of the outcome of our investigation within 30 days. If we do not respond to the complaint within 30 days, or you are not satisfied with the outcome of our investigations, you can make a complaint directly to the OAIC. Further details about how to make a complaint to the OAIC are available on the OAIC's website at www.oaic.gov.au/privacy/privacy-complaints.

Policy 1 - Open and Transparent Management of Personal Information (APP1)

DFR ensures that personal information collected as part of the ADF recruitment process is managed in an open and transparent manner. DFR implements practices, procedures and systems to ensure that:

1. it complies with the APPs; and
2. it can deal with inquiries or complaints from individuals about compliance with the APPs.

Availability of Privacy Statement

The DFR Privacy Statement is made available on the Defence Jobs website (www.defencejobs.gov.au). For access to DFR's Privacy Statement individuals are referred to the Defence Jobs website. Individuals may also request a copy of the document via email, fax or post. DFR will provide the Privacy Statement free of charge (in such a form as is appropriate).

DFR's Privacy Statement addresses all policies related to the APPs including the following key areas of personal information management;

- the kinds of personal information DFR collects and holds (refer to Policy 3);
- how DFR collects and holds personal information (refer to Policy 3 and 11);
- the purpose for which DFR collects, holds, uses and discloses personal information (refer to Policy 3 and 6);
- how an individual can access their personal information held by DFR and seek correction of their information (refer to Policy 12 and 13);
- how an individual can complain about the breach of the APP, and how DFR will deal with the complaint (refer to Policy 5 and 'Enquiries and Complaints' section); and
- DFR's disclosure of personal information to overseas recipients (refer to Policy 8).

DFR may review and update the DFR Privacy Statement from time to time, to take account of new laws or technology, or change in DFR's functions, operations and practices.

Policy 2 - Anonymity and Pseudonymity (APP2)

DFR requires that individuals identify themselves and provide their personal information to DFR in order to;

- obtain information relating to ADF careers or recruiting process. DFR may collect information and data on individuals utilising DFR managed resources (such as the Defence Jobs website);
- engage in recruiting promotions, marketing activities and research;
- make enquiries about a career or job within the ADF;

- make an application to the join the ADF; and
- engage in ADF recruiting process;

Individuals may maintain anonymity or pseudonymity for general enquiries or requests for ADF recruiting information which is made face to face, by phone, or through digital and online channels; provided that the type of information sought is general information. For further information regarding Digital Media and Electronic Tracking, refer to Policy 16.

In some circumstances, personal information such as the individual's name and email address may be requested by DFR in order to appropriately respond to the enquiry. For example: if the individual requests for information to be sent via post or fax (i.e. ADF information CD's and booklets), personal information relevant to the method in which the information is to be sent will be requested by DFR.

It is not practicable for individuals to maintain anonymity or pseudonymity with respect to making an application to join the ADF or enquiries related to their existing or pre-existing application with the ADF.

Policy 3 - Collection of Solicited Personal Information (APP3)

Collection of Personal Information

DFR solicits and collects personal information from individuals by lawful and fair means. Individuals are informed of the personal information they are required to provide to DFR and of the reasons for the solicitation of their personal information during the managed recruiting process.

Personal information collected on the Defence Jobs website (www.defencejobs.gov.au) is used for the purpose of providing individuals with information about a career in the ADF or registering an application. If an individual registers an interest, enquiry or application then information such as news, updates and promotional materials may be sent to individuals to fulfil this service.

Collection of Sensitive Information

DFR collects certain sensitive information from an individual during the managed recruiting process.

Section 6 of the *Privacy Act 1988* defines "sensitive information" as:

"(a) information or an opinion about an individual's:

(i) racial or ethnic origin; or

(ii) political opinions; or

(iii) membership of a political association; or

(iv) religious beliefs or affiliations; or

(v) philosophical beliefs; or

(vi) membership of a professional or trade association; or

(vii) membership of a trade union; or

(viii) sexual orientation or practices; or

(ix) criminal record;

that is also personal information; or

(b) health information about an individual; or

(c) genetic information about an individual that is not otherwise health information; or

(d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or

(e) biometric templates."

DFR only collects sensitive information where;

i. the individual consents to the collection of the information; and

ii. the information is reasonably necessary for or directly related to one or more of DFR's functions or activities.

DFR will not accept consent from a third-party on behalf of an individual, except where the third-party is legally authorised to represent and act on behalf of the individual. Where an individual is under the age of 18 then DFR may require and request consent from the individual's parents or legal guardian/s.

DFR will usually collect information directly from the individual, unless it is unreasonable or impracticable for it to do so. DFR may collect information from a third party with the individual's consent or where DFR is required or authorised by or under an Australian law or a court / tribunal order to collect the information from someone other than the individual. This may include personal and sensitive information such as;

- medical and psychological records;
- previous service and ADF records (where applicable);
- criminal history and police record checks;
- education, qualifications, citizenship or residency; and / or
- professional memberships (where applicable).

General Types of Information Collected

DFR will collect and maintain records and results related to an individual's eligibility and suitability for jobs within the ADF and as required for accepting, assessing, managing and progressing their application to the ADF. Personal information is collected and held by DFR through a variety of channels;

- Over the phone;

- Face to face (at Defence Force Recruiting Centres, Information Sessions or at Careers Promotional events);
- Paper and electronic forms; and
- Online and digital channels (example: Defence Jobs website and social media).

The types of personal information collected by DFR may include, as is reasonably necessary:

- Name and Biographical information;
- Demographic and statistical information;
- Contact details;
- Photograph of the individual (taken by DFR at testing sessions for identification purposes, if required);
- Citizenship information;
- Education information and results;
- Employment History information, including referee reports;
- Licences and Registrations;
- Medical and Health records and information;
- Psychological records and information;
- Previous Military Service;
- Criminal and police records;
- Testing results and records;
- Recruiting records; and
- Communications, interactions and correspondence (including preferences, opinions and feedback).

Policy 4 - Dealing with Unsolicited Personal Information (APP4)

If DFR receives unsolicited personal information about an individual then DFR will determine whether that information could have been solicited under Australian Privacy Principle 3. Where DFR determines that unsolicited personal information could have been solicited under APP 3, then DFR will treat that information in accordance with the DFR Privacy Statement and the APPs 5 to 13.

Unsolicited personal information received by DFR may be contained in or constitute a "Commonwealth record" as defined in the *Archives Act 1983*. DFR will retain that information in accordance with the requirements of that legislation, and will therefore not destroy or de-identify the information under APP 4.3.

Policy 5 - Notification of the Collection of Personal Information (APP5)

At or before the time DFR collects personal information about an individual, or as soon as reasonably practicable after collection, DFR will take reasonable steps to notify the individual or otherwise ensure the individual is aware of the matters which are required under APP 5. This includes:

- the details of the relevant law under which the collection is required (if any);
- if DFR collects personal information about the individual from another source, the fact it has done so and the circumstances of the collection;
- the main consequences (if any) for the individual if DFR does not collect the personal information; and
- the fact that DFR's Privacy Statement contains other information, including on how the individual can seek to access and correct their personal information, or make a complaint about a breach of the APPs.

Several of the matters which are required by APP 5 are addressed in this DFR Privacy Statement. Accordingly, DFR's notification under APP 5 will often be through cross-references to this APP privacy statement, including the following information.

Collection of personal information from someone other than the relevant individual

DFR may receive information about an individual (including sensitive information) from someone other than the individual for the purposes of providing its services, including;

- medical and psychological records;
- previous service and ADF records (where applicable);
- criminal history and police record checks; or
- education, qualifications, citizenship or residency;
- employment references; and
- emergency contact information.

An individual may voluntarily authorise a third-party to provide information or interact with DFR on their behalf. Common third-parties include (but aren't limited to) parents and legal guardians.

DFR will take reasonable, lawful and practicable steps to interact with authorised third-parties acting on behalf of an individual. However, to provide our services an individual is required to reasonably maintain a direct relationship with DFR.

Consequences for the individual if personal information is not collected by DFR

If DFR does not collect personal information about an individual during the recruitment process, DFR may be unable to assess the individual's eligibility and suitability for jobs within the ADF and to accept, assess, manage or progress an application to the ADF.

Policy 6 - Use or Disclosure of Personal Information (APP6)

DFR uses and discloses personal information it holds only for the purpose for which it was collected, being to provide managed recruiting services for the Australian Defence Force (ADF), including (but not limited to) marketing, research, promotion and recruiting selection processes. DFR does not use or disclose the personal information it holds for another purpose (a secondary purpose) unless;

a. the individual has consented to the use or disclosure of the information; or

b. the individual would reasonably expect that DFR use or disclose the information for the secondary purpose where;

    i. if the information is sensitive information, the secondary purpose is directly related to the primary purpose; or

    ii. if the information is not sensitive information, the secondary purpose is related to the primary purpose.

c. the use or disclosure of the information is required or authorised by or under an Australian law or Australian court/tribunal order; or

d. a "permitted general situation" as defined in section 16A of the *Privacy Act 1988* exists in relation to the use or disclosure of the information by the APP entity. This may arise where:

    i. it is unreasonable or impracticable for DFR to obtain the individual's consent, and DFR reasonably believes the use or disclosure is necessary to lessen or prevent a serious threat to the life health or safety or an individual, or to public health and safety;

    ii. DFR has reason to suspect unlawful activity or serious misconduct relating to its functions or activities, and reasonably believes the use or disclosure is necessary to permit DFR to take appropriate action in relation to the matter;

    iii. if it reasonably necessary to assist in the location of a missing person;

    iv. it is reasonably necessary to establish, exercise or defend a legal or equitable claim, or for the purposes of a confidential alternative dispute resolution process;

    v. it is necessary for DFR's diplomatic or consular functions or activities; or

    vi. DFR reasonably believes that the use or disclosure is necessary for war or warlike operations, peacekeeping or peace enforcement, or civil aid, humanitarian

assistance, medical or civil emergency or disaster relief occurring outside Australia and the external Territories; or

e. DFR reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an "enforcement body" as defined in the *Privacy Act 1988* (in which case, DFR will make a written note of the use or disclosure as required under APP 6.5); or

f. DFR discloses biometric information or biometric templates to an enforcement body in accordance with the requirements of APP 6.3.

Policy 7 – Direct Marketing (APP7)

DFR may use or disclose personal information (DFR does not use sensitive information for direct marketing purposes) for the purposes of direct marketing only if authorisation has been provided by the Commonwealth that the use or disclosure for the purposes of direct marketing is necessary in the performance of providing recruiting services on behalf of the ADF. DFR would only conduct direct marketing where;

i. the personal information was provided by the individual; and or

ii. where the individual would reasonably expect DFR to use or disclose this information for this purpose.

If DFR uses or discloses personal information for the purposes of direct marketing, or to facilitate direct marketing by any organisation, the individual may request not to receive direct marketing communications from DFR or the other organisation, and request DFR to provide its source of the information. DFR will not charge the individual for making the request or for giving effect to the request, and will notify the individual of the source of the information within a reasonable period unless it is impracticable or unreasonable to do so.

DFR may purchase third party lists. Third party suppliers can often be used by DFR's contracted agencies for the purposes of Direct Marketing.

Examples of Direct Marketing can include, but are not limited to;

- Electronic Direct Marketing (eDM);
- Direct Mail Packs;
- Newsletters; or
- Invitations.

Policy 8 - Cross Border Disclosure of Personal Information (APP8)

DFR does not disclose personal information to recipients or persons outside of Australia (not in Australia or an external Territory) and who are not the individual. If, at some point, DFR does disclose personal information to an overseas recipient it will comply with APP 8.

Policy 9 - Adoption, Use or Disclosure of Government related Identifiers (APP9)

APP9 applies to organisations only and is not applicable to DFR.

The following is provided for information only: DFR maintains a unique identifier to identify individuals which is not adopted from government related identifiers. DFR discloses its unique identifiers to the Department of Defence and individuals who have made an application to join the ADF and are participating in managed recruiting processes.

Policy 10 - Quality of Personal Information (APP10)

DFR takes reasonable steps to ensure that the personal information of individuals currently in DFR's recruiting process is accurate, up-to-date and complete, including;

- providing individuals with multiple opportunities to review the personal information collected and provide verification of its quality during the managed recruiting process;
- permitting individuals to enquire about the personal information held by DFR and advise of any amendments or corrections required to the information held (via 13 19 02 or at their closest Defence Force Recruiting Centre); and
- by requiring individuals to submit minimum standards of documentary evidence to verify their personal information.

When using or disclosing personal information to provide its services, DFR takes reasonable steps to use or disclose only accurate, up-to-date, complete and relevant information. DFR maintains dated records in accordance with Commonwealth Record Management policies and practices.

Policy 11 - Security of Personal Information (APP11)

DFR implements reasonable steps to ensure that personal information is secure and free from misuse, interference and loss and from unauthorised access, modification or disclosure. These include (but are not limited to);

- managed user access controls for digital, technical and physical resources;
- physical locks and secure storage;
- organisational security policies and processes;

- security audits and certification; and
- secure and non-public storage of personal and sensitive data and information.

Identification Verification Procedures

DFR implements identification verification procedures to take reasonable steps to ensure that unauthorised disclosure of personal information does not occur. This includes identifying individuals through a series of verification questions or other identifiable information prior to disclosing personal information over the phone or in person.

Secure Destruction and De-Identification

DFR retains records in accordance with its legal requirements, including the *Archives Act 1983*. Where destroyed, personal and sensitive information contained in DFR records, as well as recruiting documentation, is securely destroyed in accordance with Defence Security Principles Framework (DSPF).

Defence Jobs website and Online Services

DFR implements reasonable steps to protect individual's personal information collected on the Defence Jobs website and its online services against misuse, interference and loss and against unauthorised access, modification or disclosure.

Some parts on the website use SSL (Secure Sockets Layer) encryption for securing potentially sensitive or personal information. SSL is security technology that is commonly used to secure server to browser transactions. This generally includes the securing of any information passed by a browser (such as a customer's credit card number or password) to a web server (such as an online store). SSL protects data submitted over the Internet from being intercepted and viewed by unintended recipients.

While DFR strives to protect users' personal information and privacy, it cannot guarantee the security of any information collected online. If individuals are concerned about security when transmitting data over the Internet they may contact DFR via the contact methods stated in the 'Enquiry and Complaints' section of this policy.

Policy 12 - Access to Personal Information (APP12)

DFR provides individuals with access to their personal information on request by the individual, in accordance with APP 12. However, DFR may refuse to provide an individual with access to the personal information where they are required or authorised to do so under the *Freedom of Information Act 1982* or any other act of the Commonwealth or Norfolk Island enactment that provides for access by persons to documents.

The following policies apply to access to personal information;

a. The individual must make a formal request in writing for the personal information collected and/or developed during the managed recruiting process and held by DFR.

b. DFR will respond to a request for access to the personal information within 30 days after the request is made; and

c. Unless DFR is required or authorised to refuse access to the personal information as described above, DFR will give access to the information in the manner requested by the individual if it is reasonable and practicable to do so.

Access Charges

DFR does not charge a fee for individuals to access their personal information.

Refusal to Give Access

Where DFR refuses to give access to personal information, or provide access in the manner requested by the individual, then DFR will provide written notice that sets out;

a. the reasons for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable to do so; and

b. the mechanisms available to complain about the refusal; and

c. any other matter prescribed by regulations issued under the *Privacy Act 1988*.

Policy 13 - Correction of Personal Information (APP13)

DFR takes reasonable steps to correct personal information where it is satisfied that the information it holds is inaccurate, out of date, incomplete, irrelevant or misleading, or where the individual requests DFR to correct the information.

DFR will process requests to correct personal information within 30 days of receipt of request.

DFR takes reasonable steps to correct personal information previously provided to third parties, except where it would be unlawful or impracticable to do so.

Correction Charges

DFR does not charge a fee for correcting personal information.

Refusal to Correct Information

If DFR determines it is not reasonable to correct or amend personal information as requested by the individual DFR will give the individual a written notice that sets out:

a. the reasons for the refusal except to the extent that it would be unreasonable to do so; and

b. the mechanisms available to complain about the refusal; and

d. any other matter prescribed by regulations issued under the *Privacy Act 1988*.

Policy 14 - Medical Information

Candidates are required to provide DFR with medical information related to their application to the ADF. Additionally, medical personnel generate information for a candidate through medical testing and evaluation relevant to their application to the ADF.

Sensitive information is retained as 'Sensitive: Personal (Health Information)' and accessed, assessed, managed and updated by qualified Medical personnel. DFR ensures that there are reasonable restrictions and controls to ensure appropriate access to 'Sensitive: Personal (Health Information)' information only by authorised personnel.

Policy 15 - Psychological Information

Candidates are required to provide DFR with information as part of the psychological assessment undergone in determining their suitability for entry into the ADF. Authorised psychology personnel also generate information on a candidate through psychological testing and evaluation, relevant to their application with the ADF.

Sensitive information is retained as 'Sensitive: Personal (Health Information)' and accessed, assessed, managed and updated only by authorised qualified psychology personnel. DFR ensures that there are reasonable restrictions and controls to ensure appropriate access to 'Sensitive: Personal (Health Information)' information only by authorised personnel.

Policy 16 - Digital Media and Electronic Tracking

DFR utilises a range of digital and electronic technology to provide managed recruiting services for the ADF. DFR may use personal information collected through the various digital channels in an aggregated, anonymous manner for the purposes of research, but only after the information has been de-identified.

Some of the information that is collected by DFR on the Defence Jobs website is not personal information. The following sections address the type of information collected in the digital medium and the purpose of its collection.

Internet Service Provider (ISP)
When individuals visit the Defence Jobs website, DFR's Internet Service Provider (ISP) makes a record of the individual's visit. This information collected by the ISP about individuals visiting the site will not in itself identify the individual. It is collected automatically and logged due to the nature of the communication protocols.

The following information is logged for statistical purposes:

- The individuals server address;

- The individuals top-level domain name (eg. .com, .gov, .au, .uk etc.);
- The date and time of the visit to the site;
- The pages accessed and documents downloaded; and
- The previous site visited and the type of browser used.

Cookies

Some parts of the Defence Jobs website (and other online services) use cookies. The cookie allows DFR to recognise and track individual interactions with DFR's online services.

Social Media and Third Party websites

DFR utilise social media channels primarily to answer any questions and provide information on ADF careers. Personal information is not requested by DFR through social media. Any information collected by DFR via social media will be in compliance with the Terms and Conditions and Privacy Policies of the relevant social media site. DFR's current social media channels include Facebook ('Defence Jobs Australia'), YouTube, and LinkedIn.

The Defence Jobs website contains links to other sites. DFR is not responsible for the privacy practices or the content of linked websites and those sites are not covered by this Privacy Statement. Third party websites may send their own cookies to users and use other tracking devices, collect data or solicit personal information. Third party websites should have their own privacy policies, which DFR encourages users to read.

Opting out

To opt out of online and digital services managed by DFR, individuals will need to log in to their Defence Jobs account via the login link on the home page and select the 'Edit Details' link in the header. In the pop-up screen, uncheck the "I agree to receive communications from Defence Jobs" option and submit the form.

Alternatively, an individual may contact DFR to request to be opted out of services and subscriptions (via the contact details provided in this privacy statement).