



Australian Government  
Department of Immigration  
and Border Protection

**For Official Use Only**

# Use of Facebook in protection visa assessment

Interim guidance  
June 2016

Released by Department of Home Affairs  
under the Freedom of Information Act 1982

**For Official Use Only**

## Table of Contents

Table of Contents	2
Purpose	3
Introduction	3
Rationale	3
s. 47E(d)	3
Procedure	4
Obtaining access to Facebook from a CORPNET/DIMI networked desktop	4
Persona guidelines and restrictions	4
Facebook guidelines and restrictions	5
The Privacy Act	5
Passive collection	5
s. 47E(d)	5
s. 47E(d)	5
s. 47E(d)	6
Monitoring	6
Recording and storage of information	6
Procedural fairness requirements	6
s. 22(1)(a)(ii)	7

## Purpose

The purpose of this document is to provide interim guidance on accessing and using Facebook in protection visa decision making, pending the establishment of the whole-of-Department policy on social media and online collection which is currently under development.

s. 22(1)(a)(ii)

s. 22(1)(a)(ii) [@border.gov.au](https://www.border.gov.au)

## Introduction

The use of information on Facebook in protection visa decision making is a valuable way to potentially verify or refute a protection visa applicant's claimed identity or protection claims. It can be used to map relationships and memberships, provide insight into protection visa applicants' communications, locations, biometric data and related images, and gauge the veracity of applicants' claims. The use of information on Facebook increases the Department's ability to fully investigate the integrity of applicants' claims and identify applicants who may present security and character risks to the Australian community.

However, information sourced from Facebook has a range of limitations. The accuracy of information on Facebook can vary, and as such there is a need to stringently quantify its veracity for use in influencing a decision. Access to information may also be limited due to security settings on an applicant's Facebook profile.

## Rationale

Though Facebook requires users to register to access its network, the Department considers this type of information to be open source and publicly available.

Obtaining information from Facebook in protection visa decision making attracts significant risk. It is possible for Facebook administrators and other entities to track and analyse the online activity of users, which can be used to identify departmental priorities and targets.

It is, therefore, necessary to have in place guidance that supports the collection of information using Facebook whilst minimising the risk to the Department's reputation.

s. 47E(d)

s. 47E(d)

**For Official Use Only**

s. 47E(d)

## Procedure

### Obtaining access to Facebook from a CORPNET/DIMI networked desktop

The Department's IT security settings currently prevent most staff from accessing Facebook on corporate computers using their departmental logon credentials. However, it is possible to have these settings amended. Where there is an identified business need to access Facebook, such as for investigative purposes in protection visa decision making, it is possible for certain staff to gain access to Facebook to monitor activities related to their work.

Staff members who have identified a genuine business need to access Facebook must:

- gain approval from their Assistant Secretary and save it in the relevant TRIM container
- submit a request for Non Standard Internet Access through the Service Request Catalogue.

Staff members who require any level of Internet access to perform their duties must abide by the applicable departmental standards and policies, s. 22(1)(a)(ii)

s. 47E(d)

Released by Department of Home Affairs  
under the Freedom of Information Act 1982

**For Official Use Only**

s. 47E(d)

## Facebook guidelines and restrictions

### The Privacy Act

The collection of personal information from Facebook for the purposes of assessing protection visa application claims, which may include the collection of sensitive information, will be in compliance with the *Privacy Act 1988* (the Privacy Act), including the Australian Privacy Principles (APPs), as this activity is reasonably necessary for, or directly related to, one or more enforcement related activities conducted by the Department. In particular, identifying and assessing claims by non-citizens for protection in Australia. This will be so as long as the information is collected by lawful and fair means and, if the collection is from a third party, it is unreasonable or impracticable to collect the information from the individual concerned.

### Passive collection

All information collected using Facebook must only be obtained using passive collection techniques directed at public facing information only. **This means there is to be no direct contact or interaction with any other user on any social media platform.** That includes:

- 'friending' the person or others in their social media network
- commenting on a post
- 'liking' or any other 'active' action
- 'posting'
- adding photos or pictures or any other matters online
- inviting any other interaction or expressing any opinion in the online environment.

s. 47E(d)

s. 47E(d)

Released by Department of Home Affairs  
under the Freedom of Information Act 1982

**For Official Use Only**



s. 47E(d)



s. 47E(d)



When the staff member moves to a role within the Department s. 47E(d)



s. 22(1)(a)(ii)

s. 47E(d)



### Monitoring

Managers must ensure that the sites accessed by staff are appropriate and relate to current matters under consideration. Inappropriate access must be escalated to the relevant Assistant Secretary for consideration of revocation of the social media access and/or referral to Integrity and Professional Standards Branch.

s. 22(1)(a)(ii)



### Procedural fairness requirements

If the information that has been collected from Facebook would be the reason or part of the reason for refusing to grant a protection visa and is specifically about the applicant or another person and was not provided by the applicant for the purpose of the visa application, it is subject to procedural fairness requirements under s57 and s58 of the *Migration Act 1958* (the Act). Applicants must, therefore, be invited to comment on such information. There is no legal requirement, however, under s57 of the Act to disclose the source of the information unless the source of the information is itself, the adverse information on which the decision may be based.

Released by Department of Home Affairs  
under the Freedom of Information Act 1982

**For Official Use Only**



s. 22(1)(a)(ii)



**For Official Use Only**

## Use of social media in PV decision making FAQ and Reference Guide

### 1. What is social media? What is open source information?

Social media refers to websites and other online means of communication that are used by large groups of people to share information and to develop social and professional contacts.

Open source information refers to external data sources or information that is publicly available and not classified. This can include information that can be obtained by purchase, through a relationship, or through publicly accessible platforms such as media content or the internet.

### 2. Why do we use social media?

The use of information on social media in protection visa decision making is a valuable way to potentially verify or refute a protection visa applicant's claimed identity or protection claims. It can be used to map relationships and memberships, provide insight into protection visa applicants' communications, locations, biometric data and related images, and gauge the veracity of applicants' claims.

However, information sourced from social media has a range of limitations. The accuracy of information on social media can vary, and as such there is a need to stringently quantify its veracity for use in influencing a decision. Access to information may also be limited due to security settings on an applicant's social media profile.

### 3. How to use social media

s. 47E(d)

[REDACTED]

[REDACTED] Case officers must not engage with applicants through social media. s. 47E(d)

[REDACTED]

s. 22(1)(a)(ii)

s. 47E(d)

[REDACTED].

### 4. How to present adverse information located through social media to the applicant

Information obtained through social media can and should be presented to the applicant if:

- It is adverse and relates specifically to the applicant; and
- Creates concerns over their credibility (either of their claims and/or their identity) or contradicts the applicant's claims; or
- Will be referenced in the decision record for any reason as part of an adverse finding

This information must be treated as **relevant information** in line with s57 of the Migration Act.



This means that you must give the applicant an opportunity to comment of the information whether at interview or in writing through a s57 letter. Relevant response timeframes are outlined in Reg 2.15 – 7 days for invitation to respond at interview, 14 days when invitation is provided in writing.

Note however, there is no need or obligation to inform the applicant of the source of the information.

s. 22(1)(a)(ii)



s. 22(1)(a)(ii)



Released by Department of Home Affairs under the Freedom of Information Act 1982

**7. Dos and Don'ts of social media use in decision making**

<b>DO</b>	<b>DON'T</b>
Investigate the applicant's social media profile(s) to cross verify their claimed identity, affiliations, travel and associations	Assume all information on social media is accurate, reliable and true
Use this information in planning your interview lines of questioning	Draw adverse conclusions from the information presented until you have a full explanation from the applicant


Present this information to the applicant and provide them with the context / relevance of this information at interview for response (in line with s57 requirements)	Consider social media content as hard evidence
Take screen shots of content and store these in TRIM prior to the interview, noting accounts can be closed or restricted shortly after an interview	Reference information located on social media in your decision record if it has not been presented to the applicant for comment
	Engage with an applicant in any way through social media (friend, chat, comment or like posts, etc)
	Communicate, message, 'like', share or post anything on Facebook <b>S. 47E(d)</b> .
	Store or reference any social media information that is not relevant to the decision
	Refer any social media information that is not relevant to the decision to the IAA or AAT.

s. 22(1)(a)(ii)



Released by Department of Home Affairs  
under the Freedom of Information Act 1982

s. 22(1)(a)(ii)



Released by Department of Home Affairs  
under the *Freedom of Information Act 1982*

Released by Department of Home Affairs  
under the *Freedom of Information Act 1982*