AFP
AUSTRALIAN FEDERAL POLICE

FREEDOM OF INFORMATION

GPO Box 401 Canberra City ACT 2601
Telephone 02 6131 6131
Email foi@afp.gov.au
www.afp.gov.au
ABN 17 864 931 143

Our ref: CRM2016/509

29 May 2016

James Smith
Via email: foi+request-1836-13eb976e@righttoknow.org.au

Dear Mr Smith,

Freedom of Information request

I refer to your application dated 18 April 2016, under the *Freedom of Information Act 1982* (the Act) seeking the following:

> *"1. Current social media policy of the department, which covers departmental use and/or private use by employees in an individual capacity*
> *2. Any current guidance material which is available for employees to make informed decisions about their private social media use."*

Attached at Annexure A to this letter is my decision and statement of reasons for that decision. A "Schedule of Documents" identified as falling into the scope of your request is at Annexure B.

Information Publication Scheme (IPS)

As notified to you on 19 April 2016 and in accordance with section 11C of the Act, it has been decided to publish the documents in full in respect of your request. Publication of the documents and any relevant documents will be made on the AFP website at http://www.afp.gov.au/about-the-afp/information-publication-scheme/routinely-requested-information.aspx between 5 and 10 days after notification of this decision.

I apologise for the delay in processing your request and thank you for your patience.

Yours sincerely,

Nathan Scudder
Coordinator
Freedom of Information
Australian Federal Police

A

STATEMENT OF REASONS RELATING TO A FOI REQUEST BY JAMES SMITH

I, Nathan Scudder, Coordinator, Freedom of Information, am an officer authorised under section 23 of the Act to make decisions in relation to the Australian Federal Police.

What follows is my decision and reasons for the decision in relation to your application.

BACKGROUND

On 18 April 2016, this office received your application in which you requested:

> *"1. Current social media policy of the department, which covers departmental use and/or private use by employees in an individual capacity*
> *2. Any current guidance material which is available for employees to make informed decisions about their private social media use."*

SEARCHES

In relation to this request, the following searches for documents have been undertaken:

a) a search of all records held by the relevant line areas within the AFP Professional Standards; and

b) a search of all records held by the relevant line areas within the AFP.

DECISION

I have identified three documents relevant to your request. A schedule of each document and details of my decision in relation to each document is at Annexure B.

I have decided that some of the documents itemised at Annexure B are released to you with deletions pursuant to subsection 22(1)(a)(ii) the Act.

My reasons for this decision are set out below.

Further as advised to you on 16 May 2016, the AFP, as per our obligations under the Information Publication Scheme, publishes a number of documents including National Guidelines and Policies - http://www.afp.gov.au/about-the-afp/information-publication-scheme . In particular, the current version of AFP's Social Media Policy is available at http://www.afp.gov.au/~/media/afp/pdf/ips-foi-documents/ips/publication-list/afp%20policy%20-%20social%20networking.pdf and the AFP National Guideline on conflicts of interest is available at http://www.afp.gov.au/~/media/afp/pdf/ips-foi-documents/ips/publication-

list/afp%20national%20guideline%20on%20conflicts%20of%20interest%2027aug2012.pdf

Additionally, in regards to document three of your request, "*AFP National Guideline on the security of ICT system access*" only those parts relevant to social media have been released, however the document will be published on the AFP website as part of the Information Publication Scheme in due course.

WAIVER OF CHARGES

Further, given that the request has totalled only 39 pages and was not a complex request to process, I am waiving any further fees and charges which are normally associated with the processing of applications under the Act.

REASONS FOR DECISION

Folios to which subsection 22(1)(a)(ii) apply:

Subsection 22(1)(a)(ii) of the Act provides that:

> *"(1) Where:*
> *(a) an agency or Minister decides:*
> *(ii) that to grant a request for access to a document would disclose information that would reasonably be regarded as irrelevant to that request;"*

The documents or parts of documents identified in the Schedule as exempt under this section of the Act contain information which is considered irrelevant to the request. I have determined that information contained in some of the folios should be deemed to be exempt because it does not come within the scope of your application and thus falls outside the ambit of your request. By way of further explanation, these exempt folios cover information which refers to other issues which are not mentioned in your FOI application.

I find that release of the documents or parts of the documents would be an unreasonable disclosure under subsection 22(1)(a)(ii) of the Act.

EVIDENCE/MATERIAL ON WHICH MY FINDINGS WERE BASED

In reaching my decision, I have relied on the following documentary evidence:

- the scope of your application;
- the contents of the documents listed in the attached schedule;
- advice from AFP officers with responsibility for matters relating to the documents to which you sought access;
- *Freedom of Information Act 1982*;
- Guidance material issued by the Department of Prime Minister and Cabinet; and

- Guidelines issued by the Office of the Australian Information Commissioner.

***** YOU SHOULD READ THIS GENERAL ADVICE IN CONJUNCTION WITH THE LEGISLATIVE REQUIREMENTS OF THE FREEDOM OF INFORMATION ACT 1982.***

REVIEW AND COMPLAINT RIGHTS

If you are dissatisfied with a Freedom of Information decision made by the Australian Federal Police, you can apply for an internal or Information Commissioner (IC) Review. You do not have to apply for Internal Review before seeking an IC review.

You do not need to seek a review by either the AFP or the IC should you wish to complain about the AFP's actions in processing your request.

REVIEW RIGHTS under Part VI of the Act

Internal Review by the AFP

Section 53A of the Act gives you the right to apply for an internal review in writing to the Australian Federal Police (AFP) within 30 days of being notified of a decision. No particular form is required. It would assist the independent AFP decision-maker responsible for the internal review if you set out in the application, the grounds on which you consider that the decision should be reviewed.

Section 54B of the Act provides that the internal review submission must be made within 30 days. Applications for a review of the decision should be addressed to:

Freedom of Information
Australian Federal Police
GPO Box 401
Canberra ACT 2601

REVIEW RIGHTS under Part VII of the Act

Review by the Information Commissioner (IC)

Alternatively, Section 54L of the Act gives you the right to apply directly to the IC or following an internal review by the AFP. In making your application you will need to provide an address for notices to be sent (this can be an email address) and a copy of the AFP decision. It would also help if you set out the reasons for review in your application.

Section 54S of the Act provides for the timeframes for an IC review submission. For an *access refusal decision* covered by subsection 54L(2), the application must be made within 60 days. For an *access grant decision* covered by subsection 54M(2), the application must be made within 30 days.

Applications for a review of the decision should be addressed to:

Office of the Australian Information Commissioner
GPO Box 5128
Sydney NSW 2001

Further, the OAIC encourages parties to an IC review to resolve their dispute informally, and encourages agencies to consider possible compromises or alternative solutions to the dispute in this matter. The AFP would be pleased to assist you in this regard.

Information about the IC review process can be found in Part 10 of the Guidelines which are available on our website at http://www.oaic.gov.au/publications/guidelines.html.

RIGHT TO COMPLAIN under Part VIIB of the Act

Section 70 of the Act provides that a person may complain to the IC about action taken by the Australian Federal Police in relation to your application.

A complaint to the IC may be made in writing and identify the agency against which the complaint is made.

The IC may be contacted on 1300 363 992. There is no particular form required to make a complaint, but the complaint should set out the grounds on which you consider the action should be investigated.

SCHEDULE OF DECISION– CRM 2016/509
RELEASE OF DOCUMENTS – JAMES SMITH

Document No	Folio No	Date	Author	Description	Exemption	Reason
1	1-9	2/06/2015	Australian Federal Police (AFP)	Frequently asked questions (FAQ) on the use of social networking sites	**Released in part:** **Folios:** 1, 9, 22(1)(a)(ii) **Released in full:** **Folios:** 2-8	**s22(1)(a)(ii)** Exempted material would disclose information that would reasonably be regarded as irrelevant to the request.
2	10-26	2015	AFP	Personal Guide to Safety and Security	**Released in part:** **Folios:** 25, 22(1)(a)(ii) **Released in full:** **Folios:** 10-11 **Exempt in Full:** **Folios:** 12-24, 26, 22(1)(a)(ii)	**s22(1)(a)(ii)**

3	27-39		AFP	AFP National Guideline on the security of ICT system access	**Released in part:** **Folios:** 27, 35-36 22(1)(a)(ii) **Exempt in full** **Folios:** 28-34, 37-39	**s22(1)(a)(ii)**

Authorised Decision Maker:

Nathan Scudder
Coordinator
Freedom of Information
Australian Federal Police

Date of Decision: 29 May 2016

Welcome s22(1)(a)(ii)

FOR INTERNAL AFP USE ONLY

ACT Policing

National

AFP AUSTRALIAN FEDERAL POLICE Hub

Social Networking

Frequently asked questions (FAQ) on the use of social networking sites

- Does the AFP audit the online activities of its employees?
- Do I have to declare if I have an online social network account?
- Can my online presence affect my security clearance?
- Can I create and use an assumed identity (AI) on online social networking sites, in an attempt to glean information and/or evidentiary material?

Question 1. Does the AFP have a policy on the use of online social networking sites?

Yes.

The AFP Policy Statement – Online Social Networking was enacted in August 2011 and represents the AFP's position on the use of online social networking for official, operational and private purposes.

The Policy Statement should be read in conjunction with the following documents:

- AFP Code of Conduct
- National Guideline on the security of information systems

Question 2. What does the AFP class as an online social networking site?

The definition in the Policy Statement is any site that is used for the purpose of people sharing information or data with others.

Such sites include, but are not limited to: MySpace, Facebook, YouTube, Twitter, LinkedIn, Bebo, Plaxo, Flickr, Friends Reunited, Flixster, Last.fm, Xanga, Meetup.com, Bolt.com, MEETin, Tumblr etc.

Question 3. What are the risks to me if I have an online social networking account?

There are many potential risks in having a social networking account.

It can compromise your safety, the safety or your family, friends and colleagues; as well as jeopardise your future career opportunities in areas such as covert policing.

You could become a target for humiliation or fall victim to electronic scams, hacking attempts, identity theft and other fraud, physical attacks and other predatory offences such as stalking, harassment and intimidation. Some AFP appointees have already been victims to the above.

Criminals often use social networking sites to gather information on police employees and their friends, families and associates, in attempts to identify police employees who may be susceptible to corruption or intimidation. Data mining is also used by cyber thieves to extract sensitive information.

If you have a social networking account, have a look at your pages and consider:

- Would you want the material put to you while you were giving evidence?
- Could it damage your credibility/integrity?
- Would you want a selection panel to see it?
- Would you be happy for the material to be published on the front page of a

newspaper?

Remember that the founders of social networking sites often do not believe in privacy. For example, Facebook founder Mark Zuckerberg said that if he was to create Facebook again, user information would by default be public, not private.

Social networking sites incur regular cyber attacks. Below are a few examples:

- In August 2008, Facebook users were targeted by malicious hackers through postings on the popular Wall section of the site.
- In September 2008, a research and technology foundation in Greece created a small Facebook application that caused a distributed denial of service (DDOS) attack on a certain website. The application masquerades as a 'picture of the day' application and showed an image from National Geographic. However, when someone clicked on, it made a request to a victim's website. This attack ultimately pulled about 248 gigabytes of data a day from the site - essentially shutting down the server.
- In 2009, a virus swept across Facebook that sent malicious software to the user's computer, potentially stealing personal information such as addresses and telephone numbers.
- In May 2011, Sony publicly admitted that the private information of thousands of its customers, a large part derived from the use of online social networking, had been stolen by cyber thieves.

More information can be obtained from High Tech Crime Operations and www.thinkuknow.org.au.

Question 4. May I access online social networking sites at work for private use?

Yes. The AFP Policy Statement supports the philosophy of reasonable private usage.

When assessing whether usage has been reasonable, AFP management and Professional Standards will assess what the appointee's duties were at the time, the amount and intent of the usage, and whether the usage distracted the appointee from their primary duties.

For further information on "Inappropriate material" and "Prohibited use of an AFP ICT system", refer to the National Guideline on the security of information systems.

Question 5. What are the issues of accessing online social networking sites at work from AFP ICT systems?

Accessing such sites may place systems at risk of malicious attacks. Further, large amounts of private usage reduces productivity and system performance (ie: slower internet speed).

The AFP has sensitive information held on its systems and spends a large amount of time and money reducing security threats in order to protect the safety of the AFP, its information and its appointee's information.

While reasonable personal usage of AFP ICT systems is permitted, it comes at a cost to the AFP and can be more costly should a successful security cyber attack eventuate.

Question 6. May I use a personal device such as a smart phone, iPad etc, to access online social networking sites, while on duty?

Yes, but you remain subject to the provisions of the AFP Code of Conduct, the National Guideline on the security of information systems and other governance.

The AFP's expectations are that while on duty, your focus is on your work and not on private matters using personal devices. Excessive use of online social networking is a performance and possibly a conduct issue, irrespective of whether an AFP ICT system or a private device is used.

Question 7. What if through my internet usage, I become a victim of identity theft and my integrity is compromised?

Submit an integrity report **immediately** after you become aware of the event.
Wherever possible, the report should be submitted using the automated InfoPath integrity report form. If you are unable to access the automated form, the AFP Forms version should be completed and emailed to the PRS Operations Monitoring Centre (PRS OMC).

For further information on integrity reporting, refer to the AFP National Guideline on integrity reporting.

Question 8. May I use my AFP email address to create an online social networking account?

If the account is private in nature, no.

If the account is related to your official AFP duties and is sanctioned, yes.

Question 9. May I use my AFP email address as a contact on my online social networking site?

If your site is private in nature, no.

If your site is related to your official AFP duties and is sanctioned, yes.

Question 10. I am proud to be a member of the AFP. Can I upload images of myself in uniform or on duty, online?

While the AFP would prefer that you don't post any images of yourself or identify your employment status online (because of safety and associated reasons), it nonetheless trusts you to act responsibly and be fully cognisant of the personal and professional risks involved in your actions.

Ultimately, you will be held accountable for your actions should they contribute to any misconduct or other activity that warrants formal scrutiny / investigation.

Prior to loading any information into an online social networking site you must first think about how the material or images you are uploading will impact on your current and future career prospects. Identifying yourself as an AFP employee, will reduce your career opportunities in covert policing roles or other sensitive business areas.

Images uploaded to the internet can be used in numerous ways to discredit a person, threaten their integrity or steal their identity. There have been many incidents identified where AFP appointees have become victims of identify theft.

Always be cautious of taking a photograph with a Smartphone and loading the image to the internet. The image will contain metadata revealing the exact geographical location the photo

was taken, this is known as geotagging. Tagging photographs with an exact location on the Internet allows anyone to track an individual's location and correlate it with other information.

For further information on the risks of uploading material to a social networking site, refer to question 3.

Refer to question 15 for further advice on identifying yourself as an AFP appointee.

Question 11: Are there security or legal issues in uploading work related images?

Yes.

Work-related images include, but are not limited to:

- Police Operations:
  - Crime Scene images;
  - Suspect images; and
  - Images of traffic collisions
- Work-related functions where alcohol may be present.
- Images taken from both inside and around AFP premises that are not intended for an AFP media and/or marketing purpose.

There may be a security risk in the actual uploading of the images, or the images could include work areas that are subject to security restrictions.

There may also be legal or public implications in disseminating images of crime scenes or other areas that you would not have had access to, unless you were an AFP official.

If in doubt, ask a supervisor. Depending on the type of image, it may require the permission of a National Manager, prior to release.

Question 12. May I provide a reference, statement, testimonial or other type of recommendation for someone online?

It is essential to ensure any such recommendation does not compromise the integrity and effectiveness of AFP operations or impact on the confidence of the Government and the community in the integrity of the AFP and its appointees.

You must at all times be particularly mindful that any recommendations must not involve a conflict of interest or bring the AFP into disrepute.

Any reference, statement, testimonial or other type of recommendation must be in line with the National Guideline on references and testimonials.

Question 13. To protect my integrity, may I do 'policing' type checks on people I 'meet' online?

No.

Dealing with people whom you don't know in person, is an inherent risk of online social networking.

Through legislation such as the *Privacy Act 1988* the government has firmly indicated that being an AFP employee does not entitle you with privileges for private matters, beyond those enjoyed by the general public.

The personal use of AFP ICT systems is a serious breach of the professional standards of the AFP (see s.8.7 of the *AFP Code of Conduct*).

If you are concerned about someone you have met online, you should report the incident through the existing AFP reporting procedures. For guidance in those procedures, refer to the:

- AFP National Guideline on integrity reporting
- AFP National Guideline on the Security Incident Reporting Scheme

Question 14. May I use 'official information' on my online private social networking site?

No, unless you have obtained prior approval from an authorised official.

The unauthorised/inappropriate release of official information is a breach of both:

- Section 60A of the *Australian Federal Police Act 1979*; and
- The AFP Code of Conduct

Appointees are required to obtain approval in advance from the appropriate National Manager if they wish to use any information and/or experience obtained in the course of official duties. The following instruments provide advice:

- National Guideline on the security of information systems

Official AFP information - means information created or held by the AFP relating to its administration or its functions under s.8 of the *Australian Federal Police Act 1979* (Cth).

Classified information - means official information assessed and protected by classifying it according to the AFP Practical Guide on the security classification of information and is either national security classified information or non-national security classified information.

National security classified information - is official information, the compromise of which could affect the security of the nation (for example, its defence or international relations). National security classified information could be about security from espionage, sabotage, politically motivated violence, promotion of communal violence, attacks on Australia's defence system or acts of foreign interference, defence plans and operations, international relations and national interest (economic, scientific).

Non-national security classified information - is official information, the compromise of which does not threaten the security of the nation but could threaten the security or interests of individuals, groups, commercial entities, government business and interests, or the safety of the community.

Question 15. May I identify myself as an AFP appointee, online?

While in general the AFP would prefer that you don't identify your employment status online (because of safety, operational and associated reasons), it nonetheless trusts you to act responsibly and be fully cognisant of the personal and professional risks involved in your actions.

Ultimately, you will be held accountable for your actions should they contribute to any misconduct or other activity that warrants scrutiny or investigation.

Some work areas do ban employees from having an online presence, for operational reasons.

Posting identifying information online may not only compromise your safety, but also the safety of your friends, family and colleagues. As an unprecedented amount of personal information is being shared online, law enforcement personnel are becoming targets for criminal groups or individuals who intend stealing identities or identifying police employees who may be susceptible to corruption.

As an AFP appointee, you have an increased risk of identity theft.

Once information is posted on the internet, you lose control of that information. Material posted online can never really be fully deleted – it can always be found by people using certain applications and online tools.

Question 16. May I tell people online what I do in the AFP?

While in general the AFP would prefer that you didn't tell people what you do, if you are online for private purposes, it trusts appointees to both act responsibility and be fully cognisant of the personal and professional risks involved in doing so.

Remember that declaring such information could make you a target for criminal groups or foreign intelligence who are attempting to penetrate the AFP for unlawful purposes.

There are some work areas within the AFP where there are formal bans on identification (eg: Undercover Program and some parts of Protection).

Irrespective of the above, you should never provide details of operational issues such as case details, names of colleagues, shift hours etc.

Question 17. Could what I say online about the AFP, my colleagues or others, be used against me?

Yes.

Online comments are subject to the AFP Code of Conduct, criminal and civil law. You should always be mindful of the differences between personal and professional voices when making comments online. Refer to the below case studies:

Defamation

(Hunt, N., (22-11-09) Sunday Mail (SA): Teen guilty of Face book slur)

In 2009, a 19-year-old Adelaide man was convicted of criminal defamation after posting false and malicious material about a police officer on Facebook.

Breach of Code of Conduct

In April 2010 an Adelaide Coles supervisor was having a private conversation with a friend regarding a work colleague. She was angry and posted a degrading comment about the co-worker and suggested she would get what's coming to her.

The woman removed the comment - which was posted on another person's "wall" and was visible to other visitors to that page - the following day, but it had already been shown to her

management.

After being called to a meeting with her management, she realised her reference to "karma" could also be interpreted as threatening.

Even though her employer was not mentioned in the comment, Coles saw it as a breach of their company policy, and the woman was dismissed from her checkout job.

Question 18. Is it my fault if people misinterpret what I write online?

Possibly. It depends on circumstances.

Because of the nature of policing, and the high regard to which the AFP (and policing more generally) is held in the community, your comments are more likely to be interpreted as officially sanctioned if you have previously identified yourself as an AFP appointee. Alternatively, some people may feel threatened or intimidated by you because of your employment status. This may particularly be the case if you are engaged in a heated debate or argument with others.

Question 19. Isn't what I do online and in my own time, my own business?

As an AFP appointee, your off-duty actions remain subject to the professional standards framework of the AFP through the following instruments:

- Section 40RH of the *Australian Federal Police Act 1979*;
- Section 8.9 of the AFP Code of Conduct; and
- Section 8.10 of the AFP Code of Conduct.

Question 20. What if a friend or family member posts information and/or images of me on an online social networking site either with or without my consent?

If the posting is undertaken with your consent then all of the other provisions of the governance framework referred to in these FAQs apply to you, as if you had made the posting yourself.

If the posting is without your consent, and you have concerns, you should ask the friend or family member to immediately remove the posting from the site. If the posting raises issues and/or concerns about your integrity, submit an integrity report immediately (see the AFP National Guideline on integrity reporting.)

If the content of the posting shows criminal behaviour and/or a breach of the professional standards of the AFP, then the incident will be dealt with accordingly.

Question 21. Does the AFP audit online activities of its employees?

Yes.

Question 22. Do I have to declare if I have an online social networking account?

During an interview for a security clearance, you may be asked about any online social

networking that you engage in. Further, if your online social networking is part of a broader club or other group to which you are a member, that is declarable.

Question 23. Can my online presence affect my security clearance?

Yes - If your account and usage is not consistent with AFP expectations and governance.

Question 24. Can I create and use an assumed identity (AI) on online social networking sites, in an attempt to glean information and/or evidentiary material?

An AI is a fictitious identity used legitimately in support of AFP operations.

If you have an official requirement to search social websites, with an AI, it is recommended in the first instance that you seek advice from Undercover Program. The Team Leader of Undercover Services within Undercover Program is responsible for the issuing and revocation of all AFP AI's. The Team Leader can provide you advice on the usage of AI's and when they should be authorised.

AFP appointees are prohibited from creating and using an AI on social networking sites for official purposes without prior authorisation for reasons that include:

- Legal agreements that may be in place with social networking companies;
- Legislative considerations such as Part 1AC of the *Crimes Act 1914* (Cth);
- The admissibility of evidence gathered for judicial proceedings including search warrant applications; and
- Reporting obligations stemming from the following instruments:
  - AFP National Guideline on integrity reporting
  - AFP National Guideline on the Security Incident Reporting Scheme

This is an area of the law that requires careful consideration. Detailed information in relation to the acquiring and use of an assumed identity for official purposes, refer to the AFP National Guideline on assumed identities.

AFP
AUSTRALIAN FEDERAL POLICE

Personal Guide to Safety and Security

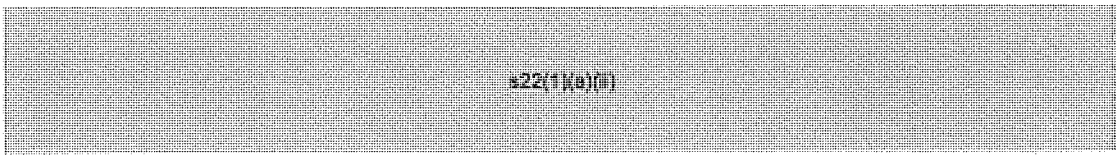
2015

AFP
AUSTRALIAN FEDERAL POLICE

Disclaimer

Each suggestion contained in this information guide is included as a guide only. It may be necessary to obtain specialist advice to meet individual circumstances and requirements. While this guide contains useful information for you and your family, it is important that you make decisions that reflect your personal circumstances. The information contained in this guide is of a general nature only and should not be considered as specialist advice.

Pages 12 through 24 redacted for the following reasons:
---
s22(1)(a)(ii)



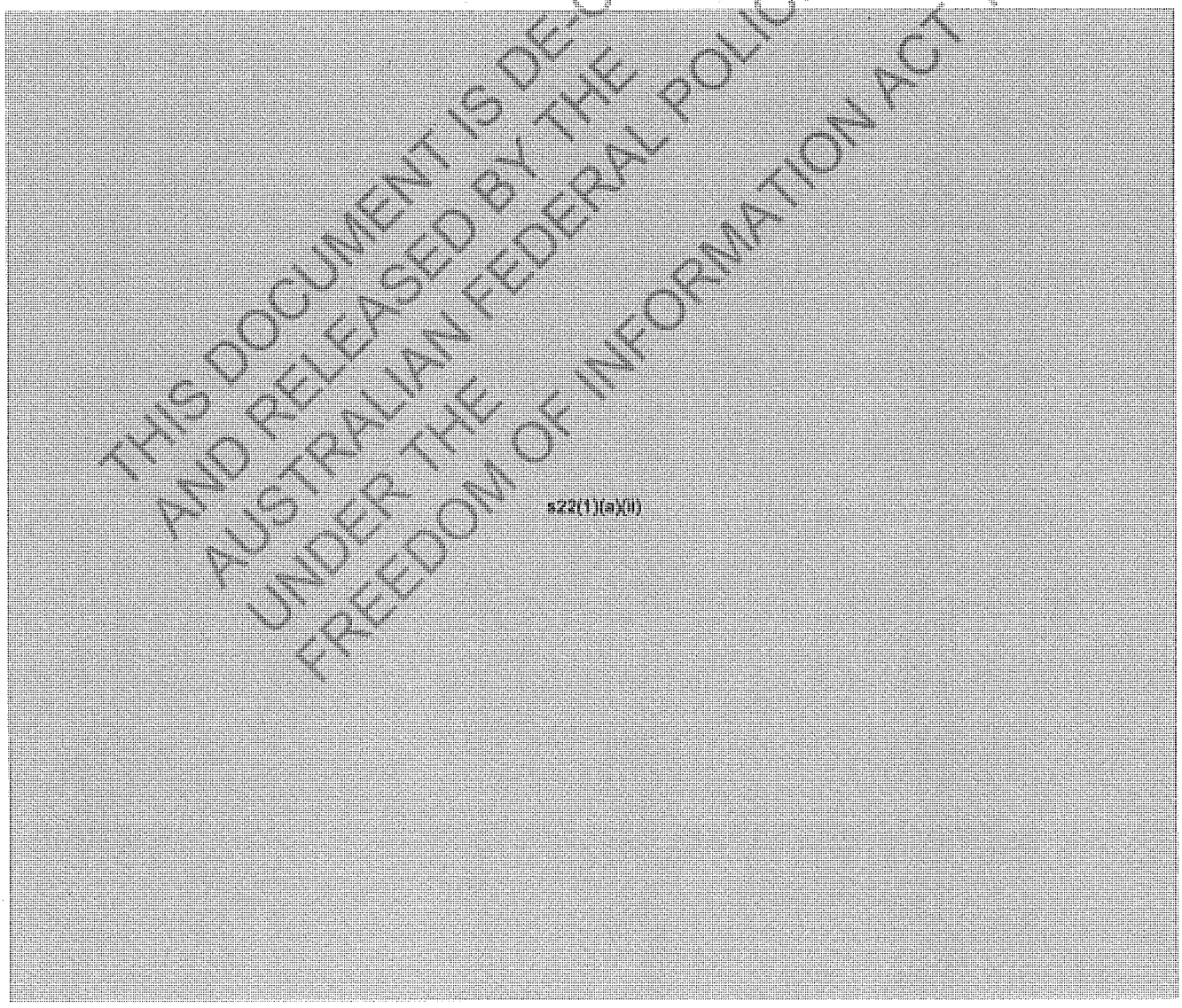
General social media considerations

Whilst social media is a valuable tool, it can compromise your safety, and the safety of your family, friends and colleagues. It can also jeopardise future career opportunities.

Individuals can become targets for humiliation or fall victim to electronic scams, hacking attempts, identity theft and other fraud, physical attacks and other predatory offences such as stalking, harassment and intimidation.

If you have a social networking account, have a look at your pages and consider:

- Would you want the material on your account presented to you while you were undertaking your professional duties?
- Could it damage your credibility/integrity?
- Would you want a selection panel to see it?
- Would you be happy for the material to be published in the public domain?

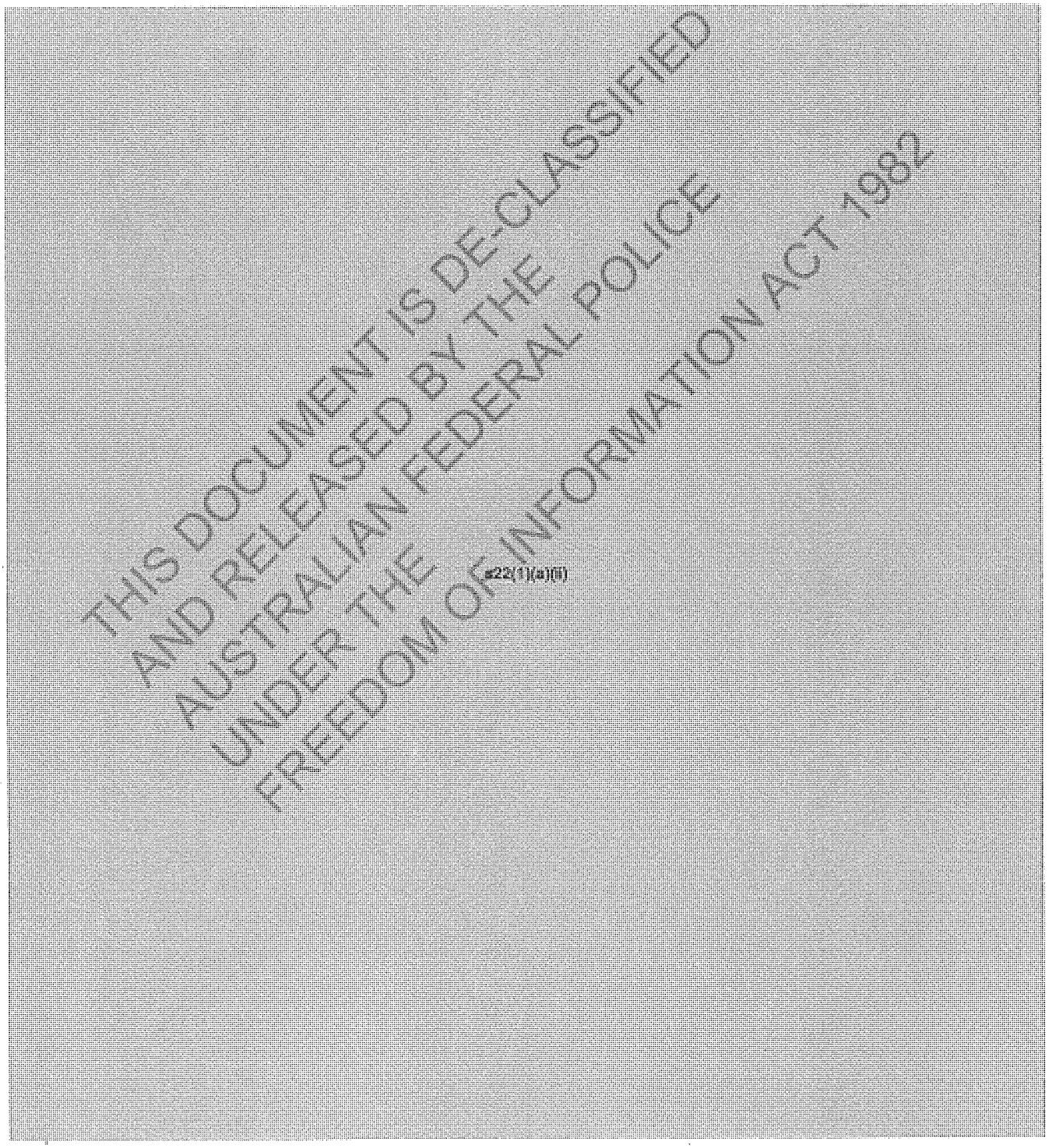


Page 26 redacted for the following reason:
---
s22(1)(a)(ii)

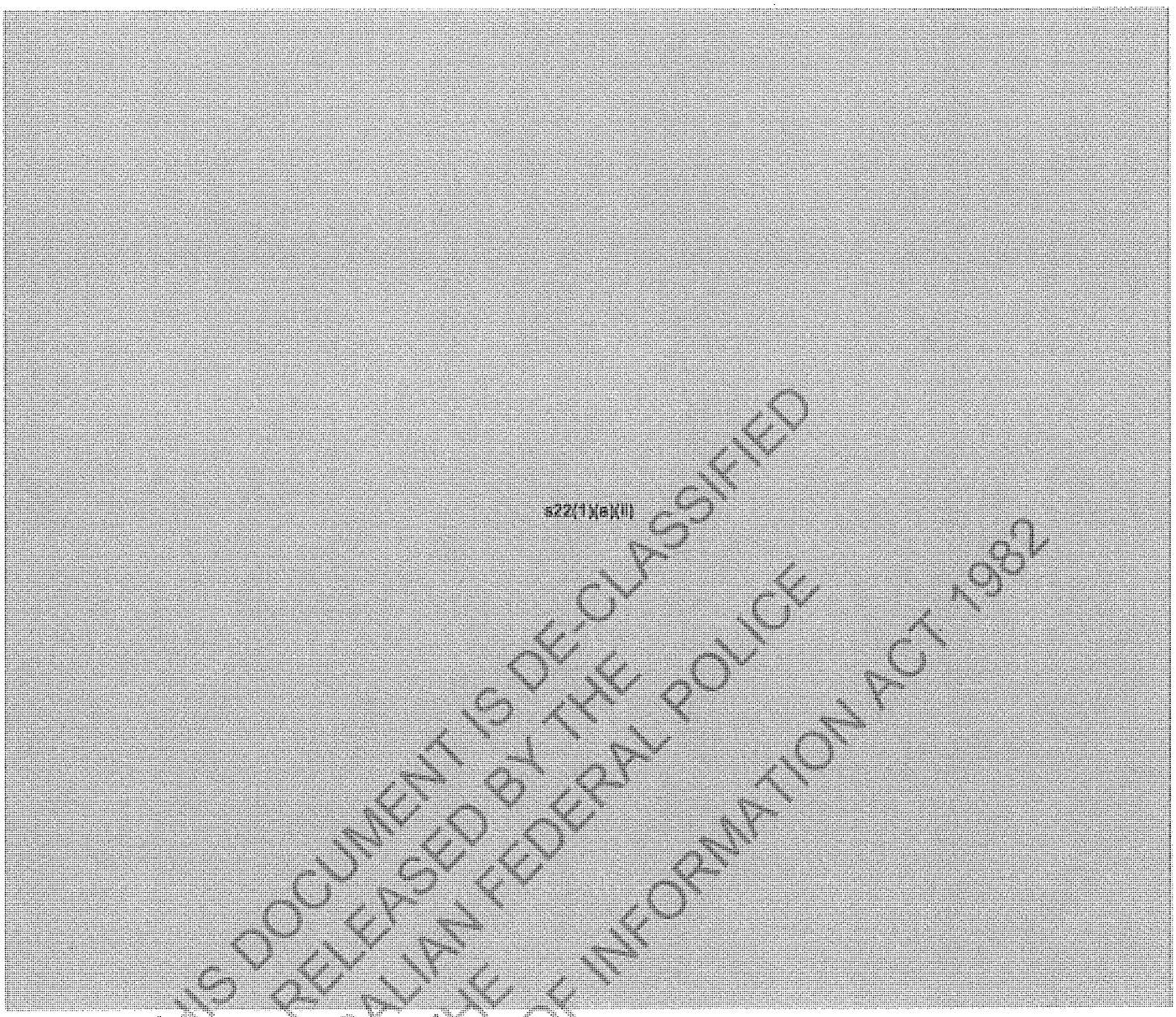
FOR INTERNAL AFP USE ONLY

AFP | Governance

AFP National Guideline on the security of information systems



Pages 28 through 34 redacted for the following reasons:
---
s22(1)(a)(ii)



17. Social networking

While system users should not identify their employment with the AFP in unofficial online social networking, the AFP trusts AFP appointees to act responsibly and mitigate risks to their safety. System users must not, however:

- establish a personal account with an AFP email address
- compromise the AFP's security, reputation or operational effectiveness
- breach s. 60A of the *Australian Federal Police Act 1979* (Cth).

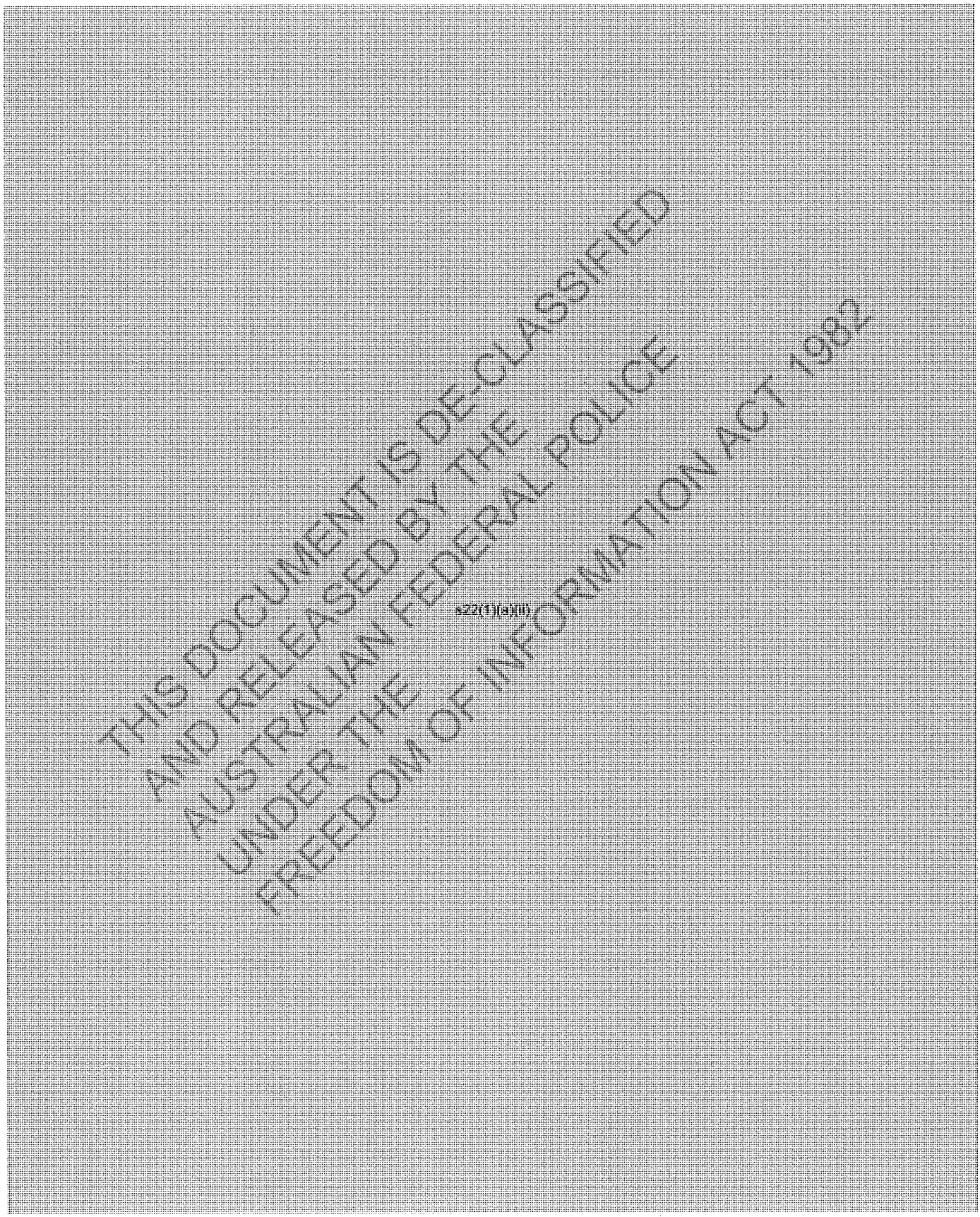
System users and their supervisors must ensure the use of social networking via personal devices whilst on duty is reasonable as per s. 8 above.

System users who publish personal information on the internet from private facilities should be aware of the security risks to themselves and to the AFP.

System users must ensure that their usage of social networking sites on AFP ICT systems does not fall outside the boundaries of acceptable use, in

accordance with s. 15 above.

Any use of AFP logos and insignia must be in accordance with the AFP National Guideline on intellectual property, commercialisation, logos and insignia.



Pages 37 through 39 redacted for the following reasons:
---
s22(1)(a)(ii)