



OFFICIAL

Detention Services Manual – Communication and engagement – Access to communication services

Procedural Instruction

Document ID (PPN)	DM-5275
TRIM Record Number	ADD2018/5121115
BCS Function	Detention Management
Document Owner	Commander, Detention Contracts, Policy and Assurance
Approval Date	04/10/2024
Document Contact	Detention Operational Policy s.22(1)(a)(ii) @abf.gov.au

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

OFFICIAL
OFFICIAL

Table of Contents

1. Purpose	Error! Bookmark not defined.
1.1. Introduction	4
2. Scope	Error! Bookmark not defined.
2.1. In Scope	Error! Bookmark not defined.
2.2. Out of Scope	4
3. Procedural Instruction	Error! Bookmark not defined.
3.1. Legislative Framework	4
The <i>Migration Act 1958</i>	4
The <i>Privacy Act 1988</i>	5
The <i>Australian Postal Corporation Act 1989</i>	5
3.2. Guiding Principles	5
3.3. Detainee access to telephone services	Error! Bookmark not defined.
Landlines	6
Mobile and internet enabled devices	7
Access to telephone services in a non-facility APOD	7
3.4. Internet access	Error! Bookmark not defined.
Terms and Conditions of Computer and Internet Use	8
Content filtering	9
ICT access and use by minors and families	10
Detainees subject to a court order	11
3.5. Detainee access to faxes	11
Access to fax machines	11
Sending a fax	12
Receiving a fax	12
3.6. Photocopying/printing services	13
Access to photocopying/printing services	13
3.7. Detainee access to mail services	13
Access to mail	13
Incoming mail	13
Sending/outgoing mail	14
Assistance with email services	14
3.8. Safety and security	14
Items that pose a risk	14
Dealing with suspected illegal, dangerous or hazardous items	15
Dealing with items that may present a risk to the IDF	15
When a detainee does not consent to opening mail	16
Taking mail offsite for further screening	17
Receiving money or valuables through the post	17
3.9. Translating and interpreting services	17
3.10. Visitors	17
3.11. Support for detainees who receive news that may adversely affect them	18

4. Accountabilities and Responsibilities

5. Version Control

Attachment A – Definitions

Attachment B – Assurance and Control Matrix

- 1.1. Powers and Obligations
- 1.2. Controls and Assurance

Attachment C – Consultation

- 1.1. Internal Consultation
- 1.2. External Consultation

Error! Bookmark not defined.

Error! Bookmark not defined.

Error! Bookmark not defined.

Error! Bookmark not defined.

Error! Bookmark not defined.

Error! Bookmark not defined.

Error! Bookmark not defined.

Error! Bookmark not defined.

Error! Bookmark not defined.

1. Purpose

1.1. Introduction

- 1.1.1. This Procedural Instruction (PI) provides guidance on detainees' access to the following communication services: email, internet, landline telephone, mobile phones, fax, photocopying and mail within the immigration detention facilities (IDFs). The Department of Home Affairs (the Department), including the Australian Border Force (ABF), and the Facilities and Detainee Service Provider (FDSP) are expected to apply these procedures consistently across the immigration detention network.
- 1.1.2. Allowing access to various types of communication services helps ensure detainees are able to communicate with family members, friends, community contacts, legal or consular representatives, other organisations or individuals and get the appropriate support they need.

2. Scope

2.1. In Scope

- 2.1.1. This PI outlines to departmental officers and contracted service providers working in an IDF the procedures for detainees' access to communication services including:
- The internet, including email.
 - Landline and mobile phones.
 - Mail services and,
 - Faxes.

2.2. Out of Scope

- 2.2.1. This PI does not cover access to communication services for detainees subject to a Residence Determination arrangement.

3. Procedural Instruction

3.1. Legislative Framework

The Migration Act 1958

- 3.1.1. Section 256 of the *Migration Act 1958* (the Migration Act), provides for detainees to have access to certain advice and facilities. This includes providing, on request, application forms for a visa, and all reasonable facilities for making a statutory declaration for the purposes of the Migration Act or for obtaining legal advice or taking legal proceedings in relation to their immigration detention.
- 3.1.2. '*All reasonable facilities*' requires the provision to a detainee of things which facilitate the obtaining of legal advice, for example, access to a telephone, to a phone book, to a fax or computer, writing materials, and a meeting room to consult with lawyers.

- 3.1.3. The Migration Act does not prohibit denying access to communication services on the basis of an individual case where there is evidence that a detainee was using communication services available in an IDF to breach the law (subject to the Department still meeting its obligations under section 256 of the Migration Act).

The Privacy Act 1988

- 3.1.4. The Department and the FDSP must not do an act, or engage in a practice that breaches the Australian Privacy Principles (APPs), as set out in Schedule 1 to the *Privacy Act 1988* (the Privacy Act). All Officers dealing with information under this PI must be aware of the Department's obligations under the APPs as well as any other relevant Australian laws relating to information handling. This includes under the Migration Act as well as the secrecy and disclosure provisions under the Australian Border Force Act 2015 where the information used as part of this PI contains Immigration and Border Protection (IBP) information.

APP 6 provides that where the Department has collected personal information about an individual for a particular purpose (primary purpose), it cannot disclose that information for another purpose (secondary purpose), unless the individual concerned consents, or an exception applies.

The Department and the FDSP may be able to use detainee user account details for:

- Monitoring and reporting of inappropriate computer and internet usage.
- Detecting activities which are potentially unlawful or are harmful to detainees or those with whom they come into contact.
- Detecting activities which would disrupt the good order of the IDF and/or,
- The purpose of preventing misuse and maintaining the integrity of the departmental Information and Communications Technology (ICT) resources.

The Australian Postal Corporation Act 1989

- 3.1.5. There are offences under the *Australian Postal Corporation Act 1989* (the APC Act), the *Criminal Code Act 1995* and the *Crimes Act 1914* which may apply to the interception and opening of mail. Refer to **3.7. Detainees access to mail services** for further guidance.

3.2. Guiding Principles

- 3.2.1. The guiding principles in relation to access to communication services in IDFs include that people in detention will be treated fairly and reasonably within the law and conditions of detention will ensure the inherent dignity of the person.
- 3.2.2. For the provision of communication services in IDFs this means that:
- Detainees will be informed during induction about access to, and conduct when, using communication services, in a language which they understand.
 - Detainees will be given reasonable access to communication services unless it presents a serious safety or security concern.
 - Detainees are encouraged to maintain reasonable contact with their family, friends, community contacts and, in the case of Immigration Guardianship of Children (IGOC) minors, their IGOC delegate.
 - Detainees are to communicate with external scrutiny bodies.

- Detainees will be afforded the same level of privacy when communicating externally as they would have in the community. Neither the Department, including the Australian Border Force (the ABF), nor the FDSP may record, intercept, read, copy or otherwise listen to a detainee's communication without their explicit consent. It is a legislative requirement of the *Australian Human Rights Commission Act 1986* (subsection 20(6)), that detainees can correspond with the Australian Human Rights Commission (AHRC) without their correspondence being opened.
- Access to the internet or other communication services may be restricted on a case-by-case basis, provided such restrictions take into account the individual circumstances of the detainee and do not interfere with the Department's obligations under section 256 of the Migration Act and that consideration is given to Australia's international obligations and,
- The FDSP is responsible for managing detainees' access to communication services while also ensuring that a detainee's rights to privacy are maintained.

3.2.3. Detainee correspondence or documentation for legal proceedings should always be prioritised, especially where it is critical that the detainee receive correspondence or documentation faxed to them by their legal representative or the relevant court or tribunal for an urgent response.

3.3. Detainee access to telephone services

Landlines

3.3.1. Communal landline telephone services for detainee use on Christmas Island are provided by the ABF. At all other IDFs, excluding non-facility alternative places of detention (APODs), the FDSP is responsible for providing communal landline telephone services for detainee use.

3.3.2. Subject to any restrictions that apply to detainees held in border screening detention (refer to *DSM – Legislative and principles overview – Border screening detention – PI (DM-589)*), detainees in IDFs can:

- Make outgoing telephone calls on communal landline telephones. Outgoing telephone calls to Australian fixed landline and Australian mobile numbers can be made at no cost to the detainee.
- Receive incoming telephone calls at all times. In most cases, incoming telephone calls will be received on a landline telephone. However, if a fixed landline telephone is not available, telephone phone calls may be received using an FDSP mobile telephone.
- Communicate with the Commonwealth Ombudsman's Office, AHRC, the Australian Red Cross, family members, legal and/or consular representatives in relation to an immigration matter at no cost and,
- Purchase phone cards of varying denominations from the FDSP operated facility shop or canteen using their Individual Allowance Program points to make international telephone calls (including international mobile calls) using the communal landline telephone service.

3.3.3. If a detainee is unable to receive a pre-booked telephone call, the officer who receives the call must maintain the privacy of the detainee by not unreasonably and/or unlawfully confirming the presence of the detainee at the IDF (all actions must be in line with the Privacy Act). Detainees must be made aware of incoming telephone calls as soon as practicable (preferably through a written message).

3.3.4. Where a pre-planned telephone call from the Commonwealth Ombudsman's Office is received, all efforts must be made by the FDSP to ensure the telephone call is facilitated.

Mobile and internet enabled devices

- 3.3.5. Detainees in an IDF are permitted to have their personal mobile and other internet enabled devices (such as iPad and tablets) in their possession. It is the detainee's responsibility to maintain service connectivity of these personal devices. Detainees are not permitted to access departmental/FDSP supplied Wi-Fi.

Access to telephone services in a non-facility APOD

- 3.3.6. Communal landline telephone services are not provided for detainee use in non-facility APODs. In a short-term APOD, such as a hotel room or medical facility, all landline telephones from the room are to be disconnected and returned to hotel reception.
- 3.3.7. The FDSP is to take all reasonable steps to ensure that detainees have reasonable access and are able to make outgoing telephone calls to Australian fixed landlines and/or Australian mobile phone numbers at no cost, commensurate with the arrangements in facility based IDFs, so far as operationally practicable.
- 3.3.8. All external requests to contact detainees must be recorded by the FDSP in the relevant log book.

3.4. Internet access

- 3.4.1. The Department and the FDSP will provide detainees with reasonable access to ICT including computer, email and internet and afford reasonable facilities for:
- Making a statutory declaration for the purposes of the Migration Act.
 - Obtaining legal advice or taking legal proceedings in relation to their immigration detention and,
 - Progressing their immigration matters.
- 3.4.2. Internet access is readily available in some IDFs, while other IDFs make use of a booking system. Most access is routine, however, in some circumstances, a detainee may require priority or out-of-hours internet access to progress their immigration case or to update family members on sensitive matters.
- 3.4.3. For routine internet access, the FDSP will:
- Assess the availability of time slots dependent on demand and,
 - Allocate detainees to time slots where a booking system is used.
- 3.4.4. For personal mobile and other internet enabled devices (such as iPad and tablets), it is the detainee's responsibility to maintain service connectivity of these personal devices. Detainees are not permitted to access departmental/FDSP supplied Wi-Fi.
- 3.4.5. If the FDSP becomes aware of, or reasonably suspects, that an incident of inappropriate use of internet and email has occurred, or that an offence in breach of Australian law has been or is being committed, the FDSP are to refer their concern/s to the ABF Superintendent (Facility) or ABF Detention Operations officers for consideration. The FDSP will make all efforts to protect its ICT through a range of measures which include, but are not limited to:

s. 47E(d)

- s. 47E(d)
- Coaching to allow detainee's to apply their best-judgement and self-agency.
- s. 47E(d)
- Physical supervision.
- s. 47E(d)
- s. 47E(d)
- Suspending or modifying (including the reduction of) internet and similar services.
- Implementing reasonable restrictions for the safety and good order of the network, detainees, departmental officers, contracted service providers and visitors and,
- Implementing any emerging or future technologies for the protection of ICT services.

3.4.6. During the induction process, detainees are to be advised of the available computer and internet services and are to be given the ABF's *'Terms and Conditions of Computer and Internet Use'* form (ADD2020/143997). The form outlines access and appropriate use of Commonwealth equipment to access the internet.

3.4.7. The FDSP will monitor the conduct of detainees using IDF computers so far as practicable without breaching personal privacy, to ensure that:

- Fairness of access to all detainees is maintained.
- The terms and conditions are adhered to and,
- Commonwealth equipment is used appropriately.

3.4.8. If the terms and conditions are not adhered to, the FDSP officer should:

- Engage with the detainee immediately.
- Discuss and reinforce the terms and conditions.
- Remove any inappropriate material from the detainee's possession and pass it on to the FDSP and,
- Document the incident in line with Incident Reporting Guidelines.

3.4.9. If a detainee breaches the terms and conditions, officers may consider implementing a Behaviour Management Plan and/or suspending computer and internet access for a prescribed period of time. For further information on behaviour management and incident reporting, refer to:

- *DSM – Safety and security management – Behaviour management – PI (DM-5027)*
- *DSM – Safety and security management – Incident management and reporting – PI (DM-616).*

Terms and Conditions of Computer and Internet Use

3.4.10. The FDSP must ensure that detainees clearly understand the expectations required of them prior to signing the ABF's *'Terms and Conditions of Computer and Internet Use'* form (ADD2020/143997). Once signed, a detainee's compliance is formally registered by the relevant FDSP officer.

3.4.11. Although a detainee **cannot** be compelled to sign the form, if they do not sign the form, the FDSP should only grant limited computer and internet access that ensures compliance with section 256 of the Migration Act (see **3.1.2.**).

- 3.4.12. What is 'limited' computer and internet access should be based on a FDSP assessment of an individual detainee's circumstances and may include a consideration and/or directive by ABF on a case by case basis, however, it would generally mean that computer and internet access for recreational purposes is not granted.
- 3.4.13. FDSP officers should record in the register whether the form has been signed/not signed and update the detainee's dossier.
- 3.4.14. In the event that a detainee declines to sign the form:
- The detainee is given a verbal advice in the first instance, including consequences for not signing the form (limited access), followed by a due date to sign.
 - Once the due date expires and the detainee has not signed the document, the FDSP officer will engage the detainee to follow up on the required action.
 - If the detainee still declines to sign after the due date, their details are to be recorded and placed on the non-compliance list and their dossier updated.
 - The FDSP must consider what computer and internet access limitations will apply to the detainee (no recreational use) until the form is signed.
- 3.4.15. For the purposes of 'limited access' a FDSP officer, in the presence of another FDSP officer, must read the terms and conditions to the detainee, with the explanation that having done so, the detainee is aware of the terms and conditions and that there are consequences if the detainee engages in conduct that contravenes the terms and conditions (where required an interpreter should be used). The FDSP officer must make a note in their notebook confirming this process has occurred, include the details of the interpreter if used and have the witnessing officer counter sign the notebook entry.
- 3.4.16. The FDSP provides a report to the ABF Detention Superintendent or delegate in each IDF at the time of the expiry of due date for signing of the forms.
- 3.4.17. For detainees entering North West Point Immigration Detention Centre (NWPIDC) on Christmas Island, the ABF's *'Terms and Conditions of Computer and Internet Use'* form (ADD2020/143997) notes that information marked with an asterisk will not apply to them. This is because the information technology arrangements in NWPIDC do not require log on to access a computer or the internet. The process is as follows:
- The detainee will be given the ABF's *'Terms and Conditions of Computer and Internet Use'* form (ADD2020/143997) in the appropriate language or using an interpreter if required.
 - The form will have an asterisk for the inapplicable content, the detainee:
 - Should be asked to initial the information with asterisks in front of the FDSP officer acknowledging the change in the form has been understood.
 - Should sign the form in the presence of the FDSP officer.
 - If detainee refuses to sign the form, refer to **3.4.14.**
 - FDSP officer records in the register that the form has been signed/not signed.
- 3.4.18. If a detainee from NWPIDC has been transferred to an IDF on the mainland, the detainee would need to be given a new form at the facility to be signed again.

3.4.19.

S. 47E(d)

3.4.20.

3.4.21.

S. 47E(d)

ICT access and use by minors and families

- 3.4.22. While minors are encouraged to access departmental ICT services in an APOD, the Department and the FDSP recognise the vulnerability of minors in the online environment. The Department and the FDSP are committed to ensuring that minors in the detention network have safe, positive experiences online, which encourages them to maintain healthy contact with their family and community contacts and promote positive mental health.
- 3.4.23. Technology is an important contributor to educational outcomes for minors. All school-aged minors will be provided with priority internet access for homework and/or educational purposes. It is the responsibility of the FDSP to prioritise internet access for school-aged minors for homework or educational purposes.
- 3.4.24. Where minors are accommodated with their families in APODs, ICT options should be made available to them in the APOD setting so that they are not required to access the designated ICT facilities in an aligned immigration detention centre. Where it is determined that school aged minors or young people are unable to attend school for health or security reasons, the FDSP should enhance and individualise ICT access for them so that they are able to complete schooling requirements without disturbance or negotiation.
- 3.4.25. Prior to signing the ABF's '*Terms and Conditions of Computer and Internet Use*' form (ADD2020/143997), the minors and their parents, guardians or carers are required to read current government informational brochures on the safe use of the internet, which will be provided by ABF Detentions Operations (Facility) or the FDSP prior to signing.
- 3.4.26. Where a minor cannot read or understand the content of the material provided, due to their language, education or developmental level, a parent, guardian or carer must read and explain the contents of the relevant material at a level and in a language suitably aimed at meeting the specific needs of that minor. ABF Detentions Operations (Facility) or the FDSP must provide this additional explanation about the content of the material to unaccompanied minors.
- 3.4.27. Only once the officer is satisfied that the above step has been completed, should they permit the minor/s to access ICT services.
- 3.4.28. All use of ICT services by minors will be logged and monitored. Monitoring online activities includes checking websites are appropriate for a minor's use, setting age-appropriate boundaries, internet limit/access software and screen time. Parents, guardians and carers should stay engaged with what the minor is accessing on the internet, monitoring the minor's behaviour particularly if their behaviour is new and out of character for them. Where practical, parents, guardians or carers should be present with a minor during ICT use and should record and monitor any suspected e-safety issues the minor experiences. Where this is not practical the FDSP must monitor the minor's behaviour noting privacy issues.
- 3.4.29. If a parent, guardian or carer is concerned about internet use or believe that it is significantly affecting the minor, they should discuss their concern with an ABF officer or contracted service provider.
- 3.4.30. When minors use computers, mobile phones and other electronic devices to access the internet and social media, breaches of privacy may lead to fraud, identity theft and unauthorised access to personal information. Other risks for minors and young people include image-based abuse

cyberbullying, trolling, stalking, online grooming, sexting, and access to inappropriate and offensive content, exposure to unreliable information or illicit materials, and invasion of online privacy.

- 3.4.31. If a minor in an APOD shows signs of engaging in inappropriate activities online, particularly if their behaviour is new and out of character for them, departmental officers and contracted service providers who work in child-related roles should talk to the minor and parent/guardian/carer about any concerns and monitor their behaviour.
- 3.4.32. Departmental officers and contracted service providers who work in child-related roles should encourage minors to report to their parents, guardians, carers or trusted adults if they encounter inappropriate content on the internet, and report the website through the *eSafety Commissioner webpage*.
- 3.4.33. Where a minor has accessed prohibited or inappropriate materials, or has been potentially compromised by contact via the internet, departmental officers and contracted service providers **must** report the incident in line with relevant departmental incident reporting procedure, refer to *DSM – Safety and security management – Incident management and reporting – PI (DM-616)* and contact the *eSafety Commissioner's office*.
- 3.4.34. For further information refer to:
- *Child Safety and Wellbeing – PS (SM-7088)*
 - *Guardianship of certain non-citizen minors – PS (VM-6457)*
 - *Best Practice for Interacting with Children – PI (BC-764)*
 - *Internet and Social Media Use for Children – SM (DM-886)* or
 - Contact the Child Wellbeing Branch at [S.22\(1\)\(a\)\(ii\)](#) @homeaffairs.gov.au.

Detainees subject to a court order

- 3.4.35. Detainees subject to a court order restricting access to the internet are **not** to be granted unrestricted internet access.
- 3.4.36. ABF Detention Operations (Facility) are to advise the FDSP of any court orders impacting detainees' access to communication services.
- 3.4.37. FDSP officers are expected to advise detainees who are subject to a court order restricting internet access that they can only access the internet in accordance with the court order and under direct supervision of FDSP officers.
- 3.4.38. **Note:** It is not the responsibility of the Department to monitor a detainee's adherence to court orders (for example, bail conditions). It is done as a matter of good practice. It is ultimately a responsibility of the detainee to adhere to the conditions imposed by the Court.

3.5. Detainee access to faxes and digital scanning device

Access to fax machines

- 3.5.1. Detainees are to be provided with reasonable access to services by the FDSP to send and receive faxes and scanned material.
- 3.5.2. Subject to restrictions that apply to detainees held in border screening detention (refer to *DSM – Legislative principles and overview - Border screening detention – PI (DM-589)*) detainees should generally be able to receive and send faxes irrespective of the destination, place of origin or time differences at no cost to themselves.

- 3.5.3. A locally approved fax register must be established by the FDSP.
- 3.5.4. All fax use (both incoming and outgoing) facilitated by the FDSP and the ABF will be noted on the FDSP Fax Register or other appropriate recordkeeping system (ABF only), as well as any issues officers and/or detainees have in sending or receiving faxes.

Sending a fax

- 3.5.5. Faxes should be sent on behalf of detainees by either an ABF or a FDSP officer during business hours. Provision should be made to fax services outside business hours if there is a critical or time-sensitive need (for example, in the preparation of a legal case or to make arrangements to leave an IDF).
- 3.5.6. When a detainee sends a personal fax, they will be required to complete a FDSP Request Form. Translating and interpreting services should be facilitated by the FDSP where required. For further information, refer to *DSM – Communication and engagement – Translating and Interpreting services – PI (DM-600)*.
- 3.5.7. Fax correspondence sent can be routine or urgent. Routine fax correspondence should be sent by the FDSP within a reasonable timeframe while urgent fax correspondence must be sent within **four (4)** business hours.
- 3.5.8. Detainee correspondence or documentation for legal proceedings should always be prioritised, especially where it is critical that the fax reaches the detainee's legal representative or the relevant court or tribunal by a set deadline. It is ultimately the detainee's responsibility to prepare correspondence/documents for legal proceedings on time. The responsibility of the FDSP is to action the request made by a detainee to send the fax in relation to their legal matters.
- 3.5.9. In cases where a fax cannot be sent by the FDSP, the FDSP officer must record the reason for the delay and provide that advice to the detainee. This is particularly important where the fax relates to immigration pathway events or decisions. Alternative arrangements should be made for sending time sensitive faxes to courts and tribunals if problems are encountered in transmission (for example, faxing from a local post office).
- 3.5.10. For privacy reasons, the content of a fax must not be read by the FDSP, except to identify the recipient.
- 3.5.11. Once a fax has been sent, the detainee will be given a copy of the transmission report and original documents by the FDSP. If a document is not faxed, the FDSP should discuss this with the detainee and record the reasons the document was not sent.
- 3.5.12. If a document is over 30 pages long and is not urgent, the detainee should be encouraged to post the document through the mail (where fax is not a requirement). Alternatively, the detainee can scan the documents and sent as an email attachment.

Receiving a fax

- 3.5.13. The FDSP will:
- Identify a designated fax number at each IDF which will be available to receive fax correspondence **24** hours a day, **seven (7)** days a week.
 - Receive, sort, envelope and deliver incoming faxes to detainees during business hours.
 - For privacy reasons, the content of a fax must not be read by the FDSP, except to identify who the fax is for.
 - Register receipt of all faxes in the FDSP Fax Register.

- Identify the intended recipient and place the fax in an envelope and label it with the detainee's details.
- Deliver faxes received for detainees by the end of the business day on which the fax is received, or on business hours the next business day if the fax is received outside core business hours and,
- Deliver any fax marked as URGENT and received outside core business hours, no later than **four (4) hours** from receipt.

3.5.14. If departmental officers receive a fax for a detainee, the fax will be placed in an envelope and, as soon as possible, provided to the FDSP for registration and delivery.

3.5.15. Each detainee is required to sign for the faxes they receive in the FDSP Fax Register. Where a detainee refuses to sign for receipt of a fax, the FDSP must document the refusal to sign.

3.6. Photocopying/printing services

Access to photocopying/printing services

3.6.1. A detainee can photocopy/print documents free of charge which:

- Are not considered controlled materials.
- Comply with relevant copyright legislation.

3.6.2. Photocopying/printing services relating to immigration pathway events or decisions are to be made available for the purposes of section 256 of the Migration Act.

3.7. Detainee access to mail services

Access to mail

3.7.1. No limit will be placed on the number of letters that a detainee can receive or send at their own expense through the mail service.

Incoming mail

3.7.2. Mail must be collected and provided to detainees daily by the FDSP (mailroom officers), except in cases of extenuating circumstances where this may not be practicable.

3.7.3. A record must be made of all incoming detainee mail in a local IDF mail register. This is the responsibility of the FDSP (mailroom officers).

3.7.4. All mail (letters, parcels and courier packages) addressed to individuals within an IDF are to be screened in order to ensure the health, safety and security of the IDF in accordance with *DSM – Safety and security management – Screening and search of vehicles, mail items and facilities SOP (DM-3290)*.

3.7.5. Officers must not open, withhold, or read mail to, or from detainees at any time, unless with permission from the detainee, or if there are safety or security concerns.

3.7.6. The details of all mail received that is unsealed or in poor condition should be recorded by the FDSP and reported to the ABF Detention Superintendent (Facility) prior to providing it to the addressee.

3.7.7. Community organisations (including advocacy groups) or individuals in the community are able to correspond with a particular detainee, only if they already have the name and address details of that detainee.

- 3.7.8. The Department, including the ABF or FDSP are not permitted to provide detainee details such as name and phone numbers to unauthorised persons making enquiries.
- 3.7.9. Mail that contains property that has been screened, confirmed as not controlled or prohibited and enters an IDF must be reflected as a transaction in the detainee's property records.
- 3.7.10. If the mail contains items that are permitted, the FDSP officer will:
- Update the detainee's property records.
 - Provide mail to the detainee and,
 - Have the detainee sign the mail received mail register.
- 3.7.11. If mail is received for a person who is no longer residing in the IDF, an ABF officer will forward the mail unopened to the forwarding address provided by the addressee or where applicable, their authorised representative. If this is not possible, the mail will be returned to the sender.

Sending/outgoing mail

- 3.7.12. Writing paper, envelopes and stamps will be available for purchase through the IDF Shop Canteen for personal use (not in relation to the obligations provided under section 256 of the Migration Act).
- 3.7.13. The FDSP officer will receive mail daily from detainee accommodation and send the mail out daily.
- 3.7.14. Detainees may ask visitors to mail items on their behalf. There are no restrictions placed around visiting third parties taking receipt of items to be mailed on behalf of detainees when they have been requested to do so and there is no concern regarding the legality of the item.
- 3.7.15. If a detainee sends a personal item through the mail, which has previously been registered as personal property with the FDSP, the item must be taken off the property register in accordance with *DSM – Managing the administration of detention – Personal property – PI (DM-598)*.
- 3.7.16. The details of all mail received that is unsealed or in poor condition should be recorded by the FDSP and reported to the ABF Detention Superintendent (Facility) prior to returning it to the detainee for resealing/packaging.

Assistance with email services

- 3.7.17. The FDSP will provide reasonable support, including organising translating and interpreting services where a detainee requests assistance in using or sending an email service for the purposes of their immigration status.

3.8. Safety and security

Items that pose a risk

- 3.8.1. Mailed items that pose a health, safety or security risk to the IDF, include:
- Any item, the possession of which is illegal.
 - A weapon or an implement that could be used to aid escape and,
 - Any item which is not permitted in IDFs.
- 3.8.2. For further information, refer to *Control of items – DSOP 64 (ADD2019/1260625)*.

3.8.3. s. 37(2)(b)

s. 37(2)(b)

3.8.4.

3.8.5.

3.8.6.

3.8.7.

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

s. 37(2)(b)

3.8.8.

3.8.9.

3.8.10.

3.8.11.

3.8.12.

3.8.13.

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

3.8.14.

3.8.15.

3.8.16.

3.8.17.

3.8.18.

s. 37(2)(b)

Receiving money or valuables through the post

- 3.8.19. Monies or valuables received through the post for a detainee should be managed in accordance with *DSM – Managing the administration of detention – Personal property – PI (DM-598)*.

3.9. Translating and interpreting services

- 3.9.1. All information provided to detainees under this instruction (oral and written) should be provided in a language that the detainee understands - either through translating important documents or by providing interpreters. This is particularly important in situations where detainees are asked to agree to a specific course of action (for example, when providing consent to open their mail in front of an officer from the FDSP or the ABF).

- 3.9.2. For further information, refer to *DSM – Communication and engagement – Translating and Interpreting services – PI (DM-600)*.

3.10. Visitors

- 3.10.1. Visitors should generally **not** have access to communication services supplied by the Department and the FDSP except where they are:

- Visiting the IDF in their capacity as a legal representative for a detainee.
- Visiting the IDF in an official capacity (for example, the Australian Red Cross) and have negotiated access through the ABF or the FDSP or it is a reasonable requirement of their visit or,
- Given permission by an ABF or FDSP officer.

- 3.10.2. For further information, refer to:

- *DSM – Legal services – Detainee access to legal representation and migration agents – PI (DM-601).*
- *DSM – Visitor Management – Visitor management – PI (DM-621).*

3.11. Support for detainees who receive news that may adversely affect them

- 3.11.1. Some detainees will receive news through the mail or through other communication services provided at an IDF that may adversely affect their behaviour. These detainees should be offered appropriate support services. Examples of news that may adversely affect a detainee include, but are not limited to:
- Decisions relating to immigration status and,
 - Personal news, such as a death in the family.
- 3.11.2. For further information, refer to *DSM – Legal services – Notification and communication of immigration decisions – PI (DM-613).*

4. Accountabilities and Responsibilities

Role	Description
Department of Home Affairs (the Department)	The Department retains ultimate responsibility for the following: • Providing reasonable access to the communication services covered in this policy, ABF's 'Terms and Conditions of Computer and Internet Use' (ADD2020/143997). • Providing reasonable facilities for communication between a detainee and their legal representative and consular representatives, police, review tribunals and other official visitors including external scrutiny bodies. • Managing detainee access to ICT services. • Managing detainee access to communication services for detainees who are in border screening detention. • Ensuring mail and other items delivered to an IDF are not withheld without reasonable cause (for example, due to safety or security concerns). • Ensuring that privacy is upheld, and the collection, use and disclosure of identifying information, personal information and Immigration and Border Protection information is in accordance with the <i>Migration Act 1958</i>, <i>Privacy Act 1988</i> and the <i>Australian Border Force Act 2015</i>. • Working with the FDSP to ensure the communication requirements of detainees in IDF are met. • Ensuring support is provided for detainees who receive news that may adversely affect them and impact on their wellbeing. The Department is responsible contractually for maintaining telephone services on Christmas Island and ensuring reasonable access for detainees.

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

Role	Description
Facilities and Detainee Services Provider (FDSP) Officer	Is responsible for: • Provision and management of communication services for detainees. • Ensuring written message/s are passed on to detainees when external telephone calls are received as soon as practical, while ensuring other detainees are not disturbed • Ensuring that all detainees have reasonable access to electronic communication. • Assisting detainees with the transmission of faxes and emails where required. • Advising and managing detainee use of the internet as per the ABF's <i>'Terms and conditions of Computer and Internet Use'</i>. • Ensuring an appropriate response should detainees not adhere to the ABF's <i>'Terms and conditions of Computer and Internet Use'</i> including: ○ Advising the detainee that continued failure to comply with the <i>'Computer and Internet Conditions of Use'</i> might result in future action, such as implementation of a Behaviour Management Plan. ○ Identifying and removing any inappropriate material and providing this material to the FDSP Security Risk Manager. The FDSP Security Risk Manager, in consultation with the FDSP Intelligence Analyst, might use this information as part of the IDF intelligence picture. ○ Ensuring that any discussions or actions are reported in the appropriate reporting mechanisms. • Ensuring that detainee requests for priority internet access are actioned and provided as soon as practical. • The prioritisation of internet access for school-age minors to complete homework or study as required and, Ensuring that detainees currently subject to a Court Order restricting internet access do not have unsupervised or unmonitored access.
FDSP	Ensure detainees are briefed on access to communication services with an IDF during reception in accordance with <i>DSM – Detainee entry and exit – Reception and induction – PI (DM-596)</i>. As part of the detainee induction process, the FDSP is to provide guidance to detainees on their rights and responsibilities regarding access to electronic communications. Specifically, the FDSP should ensure that detainees understand: • The ABF's <i>'Terms and Conditions of Computer and Internet Use'</i>. • Policy and procedures for accessing the internet; this is to include advice relating to: ○ Appropriate and inappropriate use of the internet.

Role	Description
	○ Times when the internet can be accessed, including use of any booking system that might be required in some facilities for internet access. • How to access and use fax equipment, both during and after office hours.
FDSP	Is broadly responsible for actions that are conducted after incidents within an IDF, including reporting requirements. In relation to incidents involving mail, the FDSP Duty Officer is responsible for the following: • Where a detainee refuses to open mail that is reasonably suspected to contain controlled or excluded items, ensure the items are withheld and placed in the detainee's 'in-trust' property, and raise an incident report in CCMD portal. Notify the ABF (Facility) or other available ABF officer. • Where a detainee opens mail and prohibited, excluded or controlled items are identified, ensure the items are withheld and placed in the detainee's 'in-trust' property in accordance with <i>DSM – Managing the administration of detention – Personal Property – PI (DM-598)</i>, and raise an incident report in CCMD in accordance with <i>DSM – Safety and security management - Incident management and reporting – PI (DM-616)</i>.
FDSP	Is responsible for providing mail services to detainees so that they can send and receive mail. All mail received for a detainee is to be recorded in the local mail register by the FDSP. Should mail received be suspected of containing prohibited, excluded or controlled items, FDSP are to request the mail is opened by the recipient detainee in their presence. If the detainee refuses, FDSP Officer are to report the incident immediately as per standard procedure.
FDSP	All mail entering an IDF is to be screened by FDSP. The aim of this screening is to identify any controlled or prohibited items and allow forfeiture of such items to happen in accordance with <i>Control of items – DSOP 64 (ADD2019/1260625)</i>.

5. Version Control

Version number	Date of issue	Author(s)	Brief description of change
2.0	30/06/2017	National Detention and Removal Programmes	Update of detention instructions to reflect PPT requirements.

Version number	Date of issue	Author(s)	Brief description of change
3.0	06/12/2017	National Detention and Removal Programmes	Reviewed as per Duty Commissioner's request for 'extraordinary review'.
4.0	27/06/2018	National Detention and Removal Programmes	Update post legal review (received 27/06/2018).
5.0	25/07/2018	Detention and Removal Operational Policy	Final Inspector/Superintendent review.
6.0	26/07/2018	Detention and Removal Operational Policy	Update post Superintendent review.
7.0	23/03/2021	Detention operational Policy	Updated to reflect policy change approved by Commander, National Detention Operations that detainees may make calls to Australian mobile phone numbers from landline telephone at no cost (from 29/02/2021).
8.0	21/06/2021	Detention Operational Policy	PPCF mandatory three (3) year review. Updates on: • PPCF Framework template. • Policy owner. Terminology.
9.0	04/10/2024	Detention Operational Policy	• Removal of specific job roles. • Updated references to support materials. • Inclusion of definitions page.

Attachment A – Definitions

Term	Acronym (if applicable)	Definition
Alternative place of detention	APOD	An APOD is a place of immigration detention (as defined in the Migration Act 1958) approved in writing by the Minister (or his or her delegate) under subparagraph 5(1)(b)(v) of the definition of 'immigration detention' in subsection 5(1) of the Migration Act.
Compliance, Case Management and Detention Portal	CCMD	The Compliance, Case Management and Detention Portal (CCMD) provides users easy access to CCMD material and serves as a central hub for related information. The CCMD is used by staff from a range of business areas to record and manage all visa compliance, case management and detention client data and departmental decisions. The system is also used by external service providers and the International Organization for Migration (IOM) staff with access limited to their requirements.
Facilities and Detainee Service Provider	FDSP	Contracted by the Department to provide facilities and detainee services on behalf of the Australian Government.
Immigration detention centre	IDC	Under section 273 of the Migration Act, 'detention centre' means a centre for the detention of persons whose detention is authorised under the Migration Act 1958.
Immigration detention facility	IDF	Refers to both immigration detention centres (IDC) and alternative places of detention (APOD).
Immigration Guardianship of Children delegate	IGOC delegate	An officer of the Department of Home Affairs agency who has been delegated by the Minister in the IGOC Instrument of Delegation and who is legally authorised to exercise the certain powers and functions specified under the Immigration (Guardianship of Children) Act 1946 (IGOC Act) and Instrument of Delegation with respect to an IGOC minor. See: ADF2022/394448 for the current IGOC Instrument of Delegation. For further guidance contact UHM and Guardianship section s.22(1)(a)(ii) @homeaffairs.gov.au
In-trust property		All property that the FDSP holds possession of or stores on behalf of a detainee. In addition, all excluded and controlled items are to be held as in-trust property.
Minor		Also referred to as child, is a person who is under 18 years of age. The United Nations Convention on the Rights of the Child 1989 (CRC) is an international human rights treaty setting out the fundamental human rights of children. Article

Term	Acronym (if applicable)	Definition
		of the CRC defines a child as any human being under 18 years old.
Personal property		Property belonging to a detainee is classified as either: • in-trust property. • in-possession property.
Prohibited items		Items that are considered illegal under Australian law are not permitted in any immigration detention facility (IDF).
Screening equipment		Defined in s252AA (5) of the Migration Act 1958 to mean '...a metal detector or similar device for detecting objects or particular substances'.

Attachment B – Assurance and Control Matrix

1.1 Powers and Obligations

Please Note: Staff exercising any powers, delegations or authorisations outlined in this PI (listed here) must check the latest delegation advice on the Intranet or the relevant instrument in LEGEND to ensure they currently hold the applicable power, delegation or authorisation.

Legislative Provision			Is this power delegated?	If delegated, list the relevant instruments of delegation
Legislation	Reference (e.g. section)	Section heading/provision description		
<i>Australian Border Force Act 2015</i> (ABF Act)	subsections 44(3) and 45(3)	Disclosure of Immigration and Border Protection (IBP) information	yes - authorisation	<i>Instrument of Delegation 2017</i> (DEL 17/082) (delegation applies to IBP workers of the Department of Home Affairs) <i>Australian Border Force (Secretary) No 1 of 2018</i> (ABF (s) No. 1 of 2018) (delegation applies to IBP workers in the ABF) Authorisation to disclose Immigration and Border Protection information DEL18/004 (Department of Home Affairs) Authorisation to disclose Immigration and Border Protection information ADD2020/5712705 (applies to IBP workers of the ABF excluding OSB JATF)
<i>Australian Border Force Act 2015</i> (ABF Act)	subsection 55(1)	The Secretary may, by writing, give directions to IBP workers in connection with the administration and control of the Department.	no	n/a
<i>Australian Postal Corporation Act 1989</i>	section 11A	Application of the Criminal Code 1995 (Cth)	no	n/a
<i>Criminal Code Act 1995</i>	subsections 470.1 and 470.2	Definitions Dishonesty	no	n/a

Legislative Provision			Is this power delegated?	If delegated, list the relevant instruments of delegation
Legislation	Reference (e.g. section)	Section heading/provision description		
	470.3	Determination of dishonesty to be a matter for the trier of fact		
	471.1	Theft of mail-receptacles, articles or postal messages		
	471.3	Taking or concealing of mail-receptacles, articles or postal messages		
	471.6	Damaging or destroying mail-receptacles, articles or postal messages		
<i>Crimes Act 1914</i>	sections 85E 85N 85R 85V 85Z	Interpretation – definitions Wrongful delivery of postal article etc. Wrongful delivery of postal messages Interference with property of Australia Post Articles carried by post to be taken to be Australia Post's property	no	n/a
<i>Immigration (Guardianship of Children) Act 1946</i>	subsection 5(1)	Delegation	yes	(Immigration (Guardianship of Children) Delegation (ADMIN 22/102) 2022 See: ADF2022/394448
<i>Australian Human Rights Commission Act 1986</i>	subsections 20(6, 7 & 8)	Sealed envelopes addressed to a detainee, from the Human Rights Commission, are to remain in that state upon delivery to the detainee.	no	n/a
<i>Migration Act 1958</i>	paragraph 5(1)(g)	Definition of an officer/authorised officer	yes - authorisation	<i>Migration (Migration Officers) Authorisation 2021/001 (ADMIN21/001)</i>
<i>Migration Act 1958</i>	section 256	Provides for detainees to have access to certain advice and facilities.		<i>Australian Border Force (Secretary) No 1 of 2018 (ABF (S) No. 1 of 2018)</i>

Legislative Provision			Is this power delegated?	If delegated, list the relevant instruments of delegation
Legislation	Reference (e.g. section)	Section heading/provision description		
				(delegation applies to IBP workers in the ABF) MAIDAS 10 (External Agencies)
<i>Privacy Act 1988</i>	schedule 1	Australian Privacy Principle 6 - use or disclosure of personal information	yes	n/a
<i>Public Interest Disclosure Act 2013</i>	section 7	Provides a means for protecting public officials from adverse consequences of disclosing information that, in the public interest, should be disclosed and provides for their investigation.	yes	Instrument 1 of 2020
<i>Public Service Act 1999</i>	section 13	APS Code of Conduct	no	n/a

1.2 Controls and Assurance

Related Policy	<i>Guardianship of certain non-citizen minors – PS (VM-6457)</i> <i>Records Management – PS (TI-1094)</i>
----------------	--

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

Procedures / Supporting Materials	<i>Best Practice for Interacting with Children – PI (BC-764)</i> <i>Control of items – DSOP 64 (ADD2019/1260625)</i> <i>Internet and Social Media Use for Children – SM (DM-886)</i> <i>ABF's 'Terms and Conditions of Computer and Internet Use' (ADD2020/143997)</i> <i>DSM – Visitor Management – Visitor management – PI (DM-621)</i> <i>DSM – Legislative and principles overview – Border screening detention – PI (DM-589)</i> <i>DSM – Detainee entry and exit – Reception and induction – PI (DM-596)</i> <i>DSM – Safety and security management – Behaviour management – PI (DM-5027)</i> <i>DSM – Communication and engagements – Translating and interpreting services – PI (DM-600)</i> <i>DSM – Managing the administration of detention – Personal property – PI (DM-598)</i> <i>DSM – Safety and security management – Screening and searching of detainees and their property – PI (DM-619)</i> <i>DSM – Safety and security management – Audio-visual recording – PI (DM-614)</i> <i>DSM – Legal services – Detainee access to legal representation and migration agent – PI (DM-601)</i> <i>DSM – Legal Services – Notification and communication of immigration decisions – PI (DM-613)</i> <i>DSM – Safety and security management – Incident management and reporting – PI (DM-616)</i> <i>DSM – Safety and security management – Screening and search of vehicles, mail items and facilities – SOP (DM-3290)</i>
Training/Certification or Accreditation	Nil
Other required job role requirements	Delegations Security clearance Departmental systems access
Other support mechanisms (e.g. who can provide further assistance in relation to any aspects of this instruction)	If you require further advice or assistance, or would like to provide feedback in relation to this PI, please contact the Detention Operational Policy section at s.22(1)(a)(ii) @abf.gov.au
Escalation arrangements	If you require further advice or assistance, or would like to provide feedback in relation to this PI, please contact the Detention Operational Policy section at s.22(1)(a)(ii) @abf.gov.au
Recordkeeping (e.g. system based facilities to record decisions)	Identify the approved departmental systems or facilities for record decisions or actions. For example, TRIM, ICSE, GMS, etc.

Program or Framework (i.e. overarching Policy Framework or Business Program)	Immigration Detention Facilities and Detainee Service Contract National and site-specific work instructions
Job Family Framework Role	Detention Operations Officer – Job Code 30001731

Attachment C – Consultation

1.1 Internal Consultation

The following internal stakeholders were consulted in the development of this PI:

- Humanitarian Policy and Child Wellbeing Branch
- UHM and Guardianship Section
- Detention Operations, including regional commands
- Detention Strategy and Risk Section
- Legal Group
- Privacy & Information Disclosure Section
- Status Resolution Program Management and Capability Section
- Workforce Health and Safety Section
- Detention Contracts Management Unit
- Detention Security

This policy has undergone all staff consultation in accordance with clause 1.7 of the latest Workplace Determination.

1.2 External Consultation

The following external stakeholders were consulted in the development of this PI:

- FDSP