



For Official Use Only

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

Procedural Instruction

This Procedural Instruction outlines the procedures for detainee access to communication services, including the internet, email, landline telephones, mobile phones, mail services and faxes.

Document approval date	31 July 2018
Last PPCF review date	19 February 2018
Contact details	Detention and Removals Operational Policy §. 47E(d) @abf.gov.au
Document ID (PPN)	DM-5275
TRIM record number	ADD2018/5121115
Primary influencing Legislation(s)	Migration Act 1958

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

For Official Use Only

~~For Official Use Only~~

Table of Contents

1. Introduction	4
1.1. Purpose	4
2. Scope	4
2.1. In Scope	4
2.2. Out of Scope	4
3. Glossary	4
4. Procedural Instruction	4
4.1. Guiding Principles	4
4.2. Legislative Framework	5
The Migration Act 1958	5
The Privacy Act 1988	6
The Australian Postal Corporation Act 1989	6
4.3. Detainee access to telephone services	6
Landlines	6
Mobile phones	6
Access to telephone services in a non-facility APOD	7
4.4. Internet access	7
Terms and Conditions of Computer and Internet Use	8
Content filtering	9
ICT use by minors	9
Detainees subject to a court order	10
4.5. Detainee access to faxes	10
Access to fax machines	10
Sending a fax	11
Receiving a fax	11
4.6. Photocopying services	12
Access to photocopying services	12
4.7. Detainee access to mail services	12
Access to mail	12
Incoming mail	12
Sending/outgoing mail	13
Assistance with email services	13
4.8. Safety and security	13
Items that pose a risk	13
Dealing with items that may present a risk to the IDF	14
Dealing with suspected illegal, dangerous or hazardous items	14
When a detainee does not consent to opening mail	14
Taking mail offsite for further screening	15
Receiving money or valuables through the post	16
4.9. Interpreting and translating services	16
4.10. Visitors	16
4.11. Support for detainees who receive news that may adversely affect them	16

~~For Official Use Only~~

For Official Use Only

5. Accountability and responsibilities	17
Table 1 – Procedural Instruction roles and responsibilities	17
6. Further assistance	19
7. Statement of Expectation	19
8. Related Framework documents	20
9. References and legislation	21
10. Consultation	21
10.1. Internal consultation	21
10.2. External consultation	22
11. Document details	22
11.1. Document change control	22
11.2. Procedural Instruction approval	22

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

~~For Official Use Only~~

1. Introduction

1.1. Purpose

- 1.1.1. This Procedural Instruction (PI) provides guidance on detainee access within immigration detention facilities (IDFs) to the following communication services: email, internet, landline telephone, mobile phones, fax, photocopying and mail.
- 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 and other organisations or individuals and get the appropriate support they need.

2. Scope

2.1. In Scope

- 2.1.1. This PI outlines the procedures for detainee access to communication services in IDFs including:
 - the internet, including email
 - landline telephones 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* (community placement) arrangement.

3. Glossary

- 3.1.1. The terms and their accompanying definition that have specific meaning in the context of the suite of detention instructions is at [DM-5249](#) in PPCR (*Detention Services Manual – Glossary*).

4. Procedural Instruction

4.1. Guiding Principles

- 4.1.1. The guiding principle in relation to access to communication services in IDFs is encapsulated in [DM-582](#) in PPCR (*DSM – PS – Legislative and principles overview - Service delivery values*) which states that detainees will be treated fairly and reasonably within the law and that conditions of immigration detention will ensure the inherent dignity of the person.

~~For Official Use Only~~

4.1.2. 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 are 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 IGOC minors, their Immigration Guardianship of Children (IGOC) delegate
- detainees are entitled 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 of Home Affairs (the Department), the Australian Border Force (ABF) nor the Facilities and Detainee Services Provider (FDSP) may record, intercept, read, copy or otherwise listen to a detainee's communication without their explicit invitation. It is a legislative requirement of the *Human Rights and Equal Opportunity Commission Act 1986* (s20(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 s256 of the *Migration Act 1958* (the Act), and that consideration is given to Australia's international obligations and
- the FDSP is responsible for managing and monitoring the detainees' access to communication services while also ensuring that a detainee's rights to privacy are maintained.

4.1.3. 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.

4.2. Legislative Framework

The Migration Act 1958

- 4.2.1. Section 256 of the Act, provides for detainees to have access to certain advice and facilities. This includes application forms for a visa, all reasonable facilities for making a statutory declaration for the purpose of this Act or for obtaining legal advice or taking legal proceedings in relation to their detention.
- 4.2.2. '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.
- 4.2.3. The 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 s256 of the Act).

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

~~For Official Use Only~~

The Privacy Act 1988

- 4.2.4. The Australian Privacy Principles (APPs), as set out in Schedule 1 of the *Privacy Act 1988* (the Privacy Act), allows for detainee user account details to be used by the Department, ABF and the FDSP for:
- monitoring and reporting of inappropriate computer and internet usage
 - to detect activities which are potentially unlawful or are harmful to detainees or those with whom they come into contact
 - to detect 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

- 4.2.5. There are offences under the *Australian Postal Corporation Act 1989* (APC Act), the *Criminal Code Act 1995* and the *Crimes Act 1914* which may apply to the opening and interception of mail.

4.3. Detainee access to telephone services

Landlines

- 4.3.1. 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.
- 4.3.2. Subject to any restrictions that apply to detainees held in border screening detention (refer to [DM-589](#) (*DSM - PI – Legislative and principles overview - Border screening detention*)), detainees in IDFs can:
- make outgoing telephone calls on communal landline telephones. Outgoing telephone calls to Australian fixed landline telephone numbers can be made at no cost to the detainee. Detainees may purchase a pre-paid telephone card using their Individual Allowance Program (IAP) points to make Australian mobile telephone and international telephone calls (including international mobile calls) using the communal landline telephone service
 - 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 or consular representative in relation to an immigration matter, at no cost and
 - purchase phone cards of varying denominations from the FDSP operated IDF shop or canteen
- 4.3.3. Detainees must be made aware of incoming telephone calls as soon as practicable (preferably in writing), while ensuring that other detainees are not unduly disturbed. If a detainee is unable to immediately receive a 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).
- 4.3.4. 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 phones

- 4.3.5. Detainees in an IDF are permitted to have a mobile telephone in their possession.

~~For Official Use Only~~

Access to telephone services in a non-facility APOD

- 4.3.6. 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.
- 4.3.7. The FDSP is to ensure that a mobile telephone service is available for detainees to have reasonable access to a FDSP mobile phone in order to make outgoing telephone calls to Australian fixed landline and mobile phone telephone numbers at no cost.
- 4.3.8. Each instance of a telephone call (including outgoing and incoming) will be recorded within the occurrence log by the FDSP escort officer.

4.4. Internet access

- 4.4.1. The Department, ABF and the FDSP will provide detainee's with reasonable access to ICT including computer, email and internet and afford reasonable facilities for:
 - making a statutory declaration for the purposes of the Act
 - obtaining legal advice or taking legal proceedings in relation to their immigration detention and
 - progressing their immigration claims.
- 4.4.2. 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.
- 4.4.3. 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.
- 4.4.4. The Department, ABF and the FDSP will ensure that inappropriate use of internet and email, particularly use that constitutes a breach of Australian law, is not occurring and will make all efforts to protect its ICT through a range of measures which include, but are not limited to:
 - access authentication (unique access log-ins) where possible
 - anti-virus scanning
 - blocking encrypted sessions (Secure Sockets Layers) (other than websites relevant to detainee status resolution)
 - content filtering (blocking, white or black-listing) and functionality configuration
 - coaching to allow detainee's to apply their best-judgement and self-agency
 - logging and monitoring of sessions
 - physical supervision
 - preventing some or all uploads and downloads
 - restricting certain hardware and peripherals (such as unauthorised USB sticks)
 - suspending or modifying (including the reduction of) internet and similar services
 - implementing reasonable restrictions for the safety and good order of the network, detainees, staff and visitors and
 - implementing any emerging or future technologies for the protection of ICT services.

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

~~For Official Use Only~~

- 4.4.5. During the induction process, detainees are to be advised of the available computer and internet services and are to be given a '*Terms and Conditions of Computer and Internet Use*' form. The form outlines access and appropriate use of Commonwealth equipment to access the internet.
- 4.4.6. The FDSP will monitor internet access to ensure that:
- fairness of access to all detainees is maintained
 - the terms and conditions are adhered to and
 - Commonwealth equipment is used appropriately.
- 4.4.7. If the terms and conditions is not adhered to, the FDSP officer should:
- engage with 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 Security Risk Manager and
 - document the incident in line with Incident Reporting Guidelines.
- 4.4.8. 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 Plans, refer to [DM-5027](#) in PPCR (*DSM - PI – Safety and security management - Behaviour management*).

Terms and Conditions of Computer and Internet Use

- 4.4.9. The FDSP must ensure that detainees clearly understand the expectations required of them prior to signing the '*Terms and Conditions of Computer and Internet Use*' form (the form). Once signed, detainee's compliance is formally registered by the relevant FDSP officer.
- 4.4.10. Although a detainee cannot be compelled to sign the form, if they do not sign the form, they will only be granted limited computer and internet access to ensure adherence to s256 of the Act (**see 4.2.1**) and facilitate status resolution.
- 4.4.11. What is 'limited' computer and internet access should be based on an assessment of an individual detainee's circumstances, but would generally mean that computer and internet access for recreational purposes is not granted.
- 4.4.12. FDSP officers should record in the register whether the form has been signed/not signed and update the detainee's dossier.
- 4.4.13. In the event that a detainee declines to sign the form:
- detainee is given a verbal advice in the first instance, including consequences for not signing the form (i.e. 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 (i.e. no recreational use) until the form is signed.

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

~~For Official Use Only~~

- 4.4.14. 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 used and have the witnessing officer counter sign the notebook entry.
- 4.4.15. The FDSP provides a report to the ABF Detention Superintendent in each IDF at the time of the expiry of due date for signing of the forms.
- 4.4.16. For detainees entering North West Point Immigration Detention Centre (NWPIDC) on Christmas Island, an altered version of the '*Terms and Conditions of Computer and Internet Use*' form is to be used 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 altered '*Terms and Conditions of Computer and Internet Use*' form in the appropriate language or using an interpreter if required.
 - The form will have strikethrough lines for the inapplicable content, the detainee:
 - initials the alterations 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 **4.4.13.**
 - FDSP officer records in the register that the form has been signed/not signed.
- 4.4.17. If a detainee from NWPIDC is to be transferred to an IDF on the mainland, the detainee would need to be given the unaltered version of the form to be signed again.

Content filtering

- 4.4.18. The Department, ABF or the FDSP may limit (filter) access to any web pages, or categories of webpages that are not essential to status resolution, or the access to which would breach the terms and conditions of computer and internet use.
- 4.4.19. Access to blocked sites may be granted, with approval from the FDSP. The request will be considered by the ABF Superintendent (Facility) on a case-by-case basis.
- 4.4.20. The Department, ABF and the FDSP have enabled Secure Socket Layer (SSL) interception so as to retain visibility of content within a https (internet) session and block attempts to bypass security controls or use unapproved or malicious applications.

ICT use by minors

- 4.4.21. The Department's Child Safeguarding Framework (CSF) (ADD2016/1983655) is an overarching policy framework that provides guidance and assistance to departmental staff, service providers and stakeholders to support families and children on their immigration pathway.
- 4.4.22. As a supporting material to the CSF, the '*Internet and Social Media Use for Children*' guide (ADD2017/712348) was developed. This guide is intended to support all departmental staff and contracted service providers involved in the support, care and welfare of children and their families in immigration detention and programmes.
- 4.4.23. The '*Internet and Social Media Use for Children*' guide must be implemented in conjunction with this Procedural Instruction.
- 4.4.24. While minors are encouraged to access departmental ICT services whilst in an IDF, the Department and the FDSP recognise the vulnerability and susceptibility of minors in the online environment. The Department/ABF and the FDSP are committed to ensuring that minors in the detention network have safe, positive experiences online, which encourage them to maintain healthy contact with their family and community contacts and promotes positive mental health.

~~For Official Use Only~~

- 4.4.25. Prior to signing the terms and conditions, the minor **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.
- 4.4.26. Where a minor cannot read or understand the contents 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.
- 4.4.27. Only once the officer is satisfied that the above step has been completed, should they permit the child to access ICT services.
- 4.4.28. Use of ICT services by minors will be logged and monitored. Where possible, parents, guardians and 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 possible the FDSP must supervise the minor noting privacy issues.
- 4.4.29. If a parent, guardian or carer is concerned about internet use they should discuss these issues with an ABF or contracted services provider if they believe it is significantly affecting the minor.
- 4.4.30. 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.
- 4.4.31. Where a child has accessed prohibited or inappropriate materials, or been compromised by contact via the internet, departmental staff and contracted service providers who work in child-related roles must report the incident in line with relevant departmental incident reporting procedure and must contact the Office of the eSafety Commissioner via the eSafety Hotline.

Detainees subject to a court order

- 4.4.32. Detainees subject to a court order restricting access to the internet are not to be granted unrestricted internet access.
- 4.4.33. ABF Detention Operations (Facility) are to advise the FDSP of any court orders impacting a detainee's access to communication services.
- 4.4.34. 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.

4.5. Detainee access to faxes

Access to fax machines

- 4.5.1. Detainees are to be provided with reasonable access to services by the FDSP to send and receive faxes.
- 4.5.2. Subject to restrictions that apply to detainees held in border screening detention (refer to [DM-589](#) in PPCR (*DSM - PI – Legislative principles and overview - Border screening detention*)) 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.
- 4.5.3. A locally approved fax register must be established by the FDSP.
- 4.5.4. 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/detainees have in sending or receiving faxes.

~~For Official Use Only~~

Sending a fax

- 4.5.5. 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).
- 4.5.6. When a detainee sends a personal fax, they will be required to complete a FDSP Request Form. Interpreting and translating services should be facilitated by the FDSP where required. For further information, refer to [DM-600](#) in PPCR (*DSM - PI – Communication and engagement - Interpreting and translating services*).
- 4.5.7. Fax correspondence to be sent can be routine or urgent. Routine fax correspondence is to be sent by the FDSP within a reasonable timeframe while urgent fax correspondence is to be sent within **four** business hours.
- 4.5.8. 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. This is the responsibility of the FDSP.
- 4.5.9. In cases where a fax cannot be sent by the FDSP, the FDSP officer should 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).
- 4.5.10. For privacy reasons, the content of a fax must not be read by the FDSP, except to identify who the fax is for.
- 4.5.11. Once a fax has been sent, the detainee will be given a copy of the transmission report and original documents by the FDSP officer.
- 4.5.12. 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). If a document is not faxed, the officer should discuss this with the detainee and record the reasons the document was not sent.

Receiving a fax

- 4.5.13. The FDSP officer will:
 - identify a designated fax number at each IDF which will be available to receive fax correspondence 24 hours a day, seven days a week
 - receive, sort, envelope and deliver incoming faxes to detainees during business hours
 - 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 first thing 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 hours from receipt.
- 4.5.14. If departmental staff or ABF 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.
- 4.5.15. 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.

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

For Official Use Only

4.6. Photocopying services

Access to photocopying services

- 4.6.1. A detainee can photocopy documents free of charge which:
- are not listed on the items not permitted in IDF's list or other relevant policies
 - comply with relevant copyright legislation and
 - comply with requirements relating to personal photographs.
- 4.6.2. Copies of documents relating to immigration pathway events or decisions can also be made free of charge.

4.7. Detainee access to mail services

Access to mail

- 4.7.1. 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

- 4.7.2. Mail must be collected and provided to detainees daily by the FDSP (mailroom staff).
- 4.7.3. A record must be made of all incoming detainee mail in a local IDF mail register. This is the responsibility of the FDSP (mailroom staff).
- 4.7.4. 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 [DM-3290](#) in PPCR (*DSM - SOP – Safety and security management - Screen searching vehicle, mail items, and facilities*).
- 4.7.5. At no time should any officer open, withhold or read mail to, or from, detainees except at the express invitation of the addressee or where there are safety or security concerns.
- 4.7.6. If community organisations (including advocacy groups) or individuals in the community wish to correspond with detainees, they can only do so if they already have the name and address details of the detainee. In that case they are free to address mail to that detainee.
- 4.7.7. In instances where intending correspondents do not have the name of the detainee, for privacy reasons it would be inappropriate for the Department/ABF/FDSP to provide these. In this circumstance, intending correspondents can address mail to the FDSP in the respective IDF. Where the contents of the correspondence does not contravene any legislation or detention policy settings, the FDSP may convey the contents of such correspondence to detainees.
- 4.7.8. Mail that contains property that has been screened, confirmed as not controlled or prohibited and enters an IDF must be added to the detainee's property records.
- 4.7.9. 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.
- 4.7.10. 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 addressee or where applicable, their authorised representative. If this is not possible, the mail will be returned to the sender.

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

For Official Use Only

~~For Official Use Only~~

Sending/outgoing mail

- 4.7.11. Writing paper, envelopes and stamps will be available for purchase through the IDF Canteen.
- 4.7.12. The FDSP officer will receive mail daily from detainee accommodation and send the mail out daily.
- 4.7.13. 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.
- 4.7.14. 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 [DM-598](#) in PPCR (*DSM - PI – Managing the administration of detention - Personal property*).
- 4.7.15. The details of all mail received unsealed or in poor condition should be recorded by the FDSP and provided to the ABF Detention Superintendent (Facility) and the addressee.

Assistance with email services

- 4.7.16. In the event that the FDSP receives a detainee request for assistance in using or sending an email service for the purposes of their immigration status, reasonable support, including organising interpreting and translating services will be provided by an FDSP officer.

4.8. Safety and security

Items that pose a risk

- 4.8.1. 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
 - any item, that is not permitted in IDFs.
- 4.8.2. For further information, refer to [DM-4918](#) in PPCR (*DSM - PI – Safety and security management - Items not permitted in immigration detention facilities*).

s. 47E(d)

- 4.8.4. For further information, refer to [DM-619](#) in PPCR (*DSM - PI – Safety and security management - Screening and searching of detainees and their property*) and [DM-602](#) in PPCR (*DSM - PI – Visitor management - Screening and inspection powers*).
- 4.8.5. Items suspected of posing a health, safety or security risk to the IDF should be dealt with as follows:
- the article should be separated from other mail being delivered
 - the matter should be reported immediately to the ABF Detention Superintendent (Facility)
 - an incident report should be generated as appropriate

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

~~For Official Use Only~~

- the addressee advised and action taken in accordance with Dealing with items that may present a risk to the IDF and Dealing with suspected illegal, dangerous or hazardous items.

Dealing with items that may present a risk to the IDF

- 4.8.6. If a mailed item is suspected of presenting a health, safety or security risk to the IDF but its possession is lawful (for example alcohol), the detainee must be informed that they have received an item that is suspected of presenting a health, safety or security risk to the IDF and advised that:
- they will be asked to open the mail in front of a FDSP and ABF officer
 - they have the right to refuse to open their mail (refer to when a detainee does not consent to opening mail)
 - if they do not consent to the mail being opened, then the following procedures may apply:
 - the FDSP may put the mail into secure storage which the addressee can retrieve when they leave the IDF
 - the FDSP officer may choose to open the mail without the addressee's consent (refer to when a detainee does not consent to opening mail)
 - if items are found that breach Commonwealth, state or territory laws, the police will be involved.
- 4.8.7. Once the addressee has been advised of the above, they should be asked if they wish to have a support/independent person present. If the detainee is a minor they should be accompanied by their parent or guardian. An interpreter should be used if necessary.

Dealing with suspected illegal, dangerous or hazardous items

- 4.8.8. If there is a suspicion or a discovery that the mail contains items that are illegal, dangerous or hazardous, the following action are to be taken:
- the police and appropriate emergency services should be informed and requested to take possession of the item
 - in the meantime, the item must be handled in accordance with any police advice, until the relevant emergency services arrive
 - the FDSP should take the advice of the police as to whether to inform the detainee about the mailed item
 - all hazardous or dangerous items should be handled in accordance with the appropriate Occupational Health and Safety guidelines.

When a detainee does not consent to opening mail

- 4.8.9. If the detainee does not consent to opening mail, the FDSP officer should reassess the risk of the mail on the basis of:
- the nature of the item believed to be in the mail
 - possible consequences if the item is allowed into the IDF
 - possible consequences if the mail is not opened and
 - any discussions the Department, ABF, FDSP and the detainee have had about the nature of the mail.

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

~~For Official Use Only~~

- 4.8.10. If the FDSP officer still has concerns that the item may be inappropriate but does not present an immediate health, safety and security risk to the IDF, they may give the detainee up to 24 hours to reconsider opening the mail in front of them. During this time the mail should be placed in confiscated in-trust storage and the detainee informed that the item is in storage.
- 4.8.11. If the detainee does not give consent to open the mail following the 24-hour period and it is believed the item does not present an immediate health, safety and security risk to the IDF then the FDSP should place the mail in confiscated in-trust storage, which the detainee may retrieve when they leave the IDF. The detainee to whom the mail is addressed should be given a property receipt for the item and the incident should be recorded as appropriate.
- 4.8.12. If the item is considered to be a serious or imminent threat to the safety and security of the IDF, a joint decision will be made between the FDSP Facility Operations Manager (FOM) and the ABF Detention Superintendent (Facility) as to whether the mail is to be opened. Consideration may be given to seeking legal guidance in this regard. In making this decision **ALL** of the following conditions are to be met:
- the FDSP officer has well-founded reasons to suspect that, even in secure storage, the item presents a serious and imminent threat to the safety and security of the IDF
 - there are reasonable indicators of this risk (see reasons to suspect mail above)
 - opening the mail would be a fair and reasonable act to ensure the safety and security of the IDF
 - the detainee to whom the mail is addressed has been given every reasonable opportunity to open their own mail
 - all other reasonable options to find out the contents of the mail have been exhausted.
- 4.8.13. The decision should be appropriately recorded and the detainee informed of the decision and given a final opportunity to open the mail. Any action taken by the FDSP officer should be in the presence of:
- an ABF officer
 - the addressee detainee and
 - if requested by the addressee detainee, an independent/support person.
- 4.8.14. All action taken in relation to mail suspected of presenting a risk to the IDF must be fully documented.
- 4.8.15. The FDSP should video record the incident, to ensure a visual record is maintained. The decision to video record the incident and the reasoning on which it was based must be recorded in writing.
- 4.8.16. For further information, refer to [DM-614](#) in PPRC (*DSM – PI – Safety and security management – Audio-visual recording*).

Taking mail offsite for further screening

- 4.8.17. Where detainee mail is suspected of containing a prohibited, excluded or controlled item, it should only be sent offsite for further screening if:
- the detainee has been asked to open the mail in front of ABF and FDSP officers; and
 - the detainee consents to opening the mail and it is found to contain an unidentifiable item; and
 - ABF and FDSP officers continue to believe that the unidentifiable item is a prohibited, excluded or controlled item, and
 - the detainee consents to the item being sent offsite for further screening.

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

~~For Official Use Only~~

- 4.8.18. If the detainee does not consent (to the mail being opened as an initial step or to an unidentified item found within the mail being sent offsite for screening), the mail should be stored as in-trust property (assuming it is not considered to pose a serious or imminent threat).

Receiving money or valuables through the post

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

4.9. Interpreting and translating services

- 4.9.1. 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).
- 4.9.2. For further information, refer to [DM-600](#) (*DSM - PI – Communication and engagement - Interpreting and translating services*).

4.10. Visitors

- 4.10.1. Visitors should generally not have access to communication services supplied by the Department, ABF and the FDSP except where they are:
- visiting legal representatives
 - visiting in a professional capacity (for example, the Australian Red Cross) and have negotiated access through the ABF or the FDSP FOM or it is a reasonable requirement of their visit or
 - given permission by an ABF or FDSP officer.
- 4.10.2. For further information, refer to:
- [DM-601](#) in PPCR (*DSM - PI – Legal services - Detainee access to legal representation and migration agents*)
 - [DM-621](#) in PPCR (*DSM - PI – Visitor management - Visitor management*).

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

- 4.11.1. Detainees who receive advice that may adversely affect them through the mail or through other communication services provided at an IDF must be offered appropriate support. 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.
- 4.11.2. For further information, refer to [DM-613](#) in PPCR (*DSM - PI – Legal services - Notification of immigration decisions*).

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

For Official Use Only

5. Accountability and responsibilities

Table 1 – Procedural Instruction roles and responsibilities

Position	Accountability and/or responsibility
Department of Home Affairs	<p>The Department retains ultimate responsibility for the following:</p> <ul style="list-style-type: none"> providing reasonable access to the communication services covered in this policy, 'Terms and Conditions of Computer and Internet Use' form and the Department's duty of care obligations. See DM-583 in PPCR (DSM - PS – Legislative and principles overview - Duty of care to detainees) providing reasonable facilities for communication between a detainee and their legal representative and consular representatives, 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 personal information is in accordance with the <i>Migration Act 1958</i> and <i>Privacy Act 1988</i> working with the FDSP to ensure the communication requirements of detainees in IDF are met providing support for detainees who receive news that may adversely affect them and impact on their wellbeing. <p>The Department is responsible contractually for maintaining telephone services on Christmas Island and ensuring reasonable access for detainees.</p>
FDSP Officer	<p>Are responsible for:</p> <ul style="list-style-type: none"> provision, monitoring and management of communication services for detainees ensuring detainees are made aware of incoming telephone calls 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 monitoring detainee use of the internet as per the 'Terms and conditions of Computer and Internet Use' form ensuring an appropriate response should detainees not adhere to the "Terms and conditions of Computer and Internet Use" form including:

For Official Use Only

For Official Use Only

Position	Accountability and/or responsibility
	<ul style="list-style-type: none"> ○ advising the detainee that continued failure to comply with the 'Computer and Internet Conditions of Use' 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. s. 47E(d) ○ ensuring that any discussions or actions are reported in the appropriate reporting mechanisms. <ul style="list-style-type: none"> • ensuring that detainee requests for priority internet access are actioned and provided as soon as practical • the prioritisation of internet access for school-age children 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 Reception Officer	<p>FDSP Reception Officer provides the first point of contact between FDSP officers and detainees.</p> <p>Ensure detainees are briefed on access to communication services within an IDF during reception in accordance with <i>DM-596</i> in PPCR (<i>DSM - PI – Detainee entry and exit - Reception and induction</i>)</p> <p>As part of the detainee induction process, FDSP Reception Officer are to provide guidance to detainees on their rights and responsibilities in regards to access electronic communications.</p> <p>Specifically, FDSP Reception Officer should ensure that detainees understand:</p> <ul style="list-style-type: none"> • the 'Terms and Conditions of Computer and Internet Use' form • policy and procedures for accessing the internet; this is to include advice relating to: <ul style="list-style-type: none"> ○ appropriate and inappropriate use of the internet ○ 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 Facility Operations Manager (FOM) / FDSP Duty Manager	<p>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:</p> <ul style="list-style-type: none"> • 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 trust property, and raise an incident report in CCMD. Notify the ABF Security Liaison Officer or other available ABF officer • where a detainee opens mail and prohibited, controlled or excluded items are identified, ensure the items are withheld and placed in the

For Official Use Only

Position	Accountability and/or responsibility
	detainee's trust property in accordance with DM-4918 in PPCR (<i>DSM - PI – Safety and security management - Items not permitted in immigration detention facility</i>), and raise an incident report in CCMD in accordance with DM-616 in PPCR (<i>DSM - PI – Safety and security management - Incident Management and reporting</i>).
FDSP Mailroom Officer	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 Mailroom Officer. Should mail received be suspected of containing excluded or controlled items, FDSP Mailroom Officer are to request the mail is opened by the recipient detainee in their presence. If the detainee refuses, FDSP Mailroom Officer are to advise the FDSP FOM immediately.
FDSP Screening Officer	All mail entering an IDF is to be screened by FDSP Screening Officer. The aim of this screening is to identify any controlled or prohibited items and allow forfeit of such items to happen in accordance with DM-4918 in PPCR (<i>DSM - PI – Safety and security management - Items not permitted in immigration detention facility</i>).

6. Further assistance

- 6.1.1. If you require further advice or assistance, or would like to provide feedback in relation to this PI, please contact the Detention and Removal Operational Policy section at [s. 47E\(d\)](#) @abf.gov.au.

7. Statement of Expectation

- 7.1.1. The APS Code of Conduct states that 'an APS employee must comply with any lawful and reasonable direction given by someone in the employee's Agency who has authority to give the direction' (subsection 13(5) of the *Public Service Act 1999* (Public Service Act)).
- 7.1.2. Failure by an APS employee to comply with any direction contained in a PPCF document may be determined to be a breach of the APS Code of Conduct, which could result in sanctions up to and including termination of employment, as set out in subsection 15(1) of the Public Service Act.
- 7.1.3. The Secretary's Professional Standards Direction, issued under subsection 55(1) of the *Australian Border Force Act 2015* (the ABF Act), requires all IBP workers who are not APS employees (such as contractors or consultants) to comply with any lawful and reasonable direction given by someone in the Department with authority to issue that direction.
- 7.1.4. Failure by an IBP worker who is not an APS employee to comply with a direction contained in a PPCF document may be treated as a breach of the Professional Standards Direction, which may result in the termination of their engagement under section 57 of the ABF Act. Non-compliance may also be addressed under the terms of the contract engaging the contractor or consultant.

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

~~For Official Use Only~~

- 7.1.5. For all other provisions of PPCF documents, the Secretary and the Commissioner ABF expect all IBP workers to:
- consider whether a proposed departure from any provision set out in a PPCF document is reasonable and justified in the circumstances
 - consider the risks of departing from any provision set out in a PPCF document
 - be responsible and accountable for the consequences of departing from, or not adhering to the content of, all PPCF documents, including where such departure or non-adherence results in a breach of any legal or other obligations which lead to adverse outcomes for the Department and
 - be responsible for documenting the reasons/justification for their decision to depart from, or not adhere to, any PPCF document.
- 7.1.6. IBP workers who make decisions or who exercise powers or functions under legislation have a duty to make these decisions or exercise these powers or functions in accordance with the requirements of the legislation and legal principle.

8. Related Framework documents

8.1.1. Related Framework documents include:

- [DM-582](#) in PPCR (DSM - PS - Legislative and principles overview - Service delivery values)
- [DM-589](#) in PPCR (DSM - PI - Detainee placement - Border screening detention)
- [DM-4918](#) in PPCR (DSM - PI - Safety and security management - Items not permitted in IDF)
- [DM-600](#) in PPCR (DSM - PI - Communication and engagements - Interpreting and translating services)
- [DM-598](#) in PPCR (DSM - PI – Managing the administration of detention - Personal property)
- [DM-619](#) in PPCR (DSM - PI – Safety and security management - Screening and searching of detainees and their property)
- [DM-4927](#) in PPCR (DSM - PI - Visitor management - Screening and inspection powers)
- [DM-614](#) in PPCR (DSM - PI – Safety and security management - Audio-visual recording)
- [DM-601](#) in PPCR (DSM - PI – Legal services – Detainee access to legal representation and migration agent)
- [DM-621](#) in PPCR (DSM - PI – Visitor management - Visitor management)
- [DM-613](#) in PPCR (DSM - PI – Legal Services - Notification of immigration decisions)
- [DM-596](#) in PPCR (DSM - PI – Detainee entry and exit – Reception and induction)
- [DM-616](#) in PPCR (DSM - PI – Safety and security management - Incident Management and reporting)
- [DM-583](#) in PPCR (DSM - PS – Legislative and principles overview - Duty of care to detainees)
- [DM-3290](#) in PPCR (DSM - SOP – Safety and security management - Screen searching vehicle, mail items, and facilities)
- [DM-5027](#) in PPCR (DSM - PI – Safety and security management - Behaviour management)
- [DM-602](#) in PPCR (DSM - PI – Visitor management - Screening and inspection powers)

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

~~For Official Use Only~~

- [DM-5249](#) in PPCR (*Detention Services Manual – Glossary*) Child Safeguarding Framework (ADD2016/1983655)
- Internet and Social Media Use for Children Guide (ADD2017/712348)
- Reporting Child-related Incidents Policy
- IDN critical incident communication framework (ADD2016/1786320)
- Terms and Conditions of Computer and Internet Use (ADD2017/3810605)
- National and site specific work instructions

9. References and legislation

9.1.1. References and legislation include:

- *Australian Border Force Act 2015*
- Australian Public Service Code of Conduct
- Article 17 of the International Covenant on Civil and Political Rights
- Immigration Detention Facilities and Detainee Services Contract
- *Migration Act 1958*
- *Privacy Act 1988*
- Mandatory reporting of serious misconduct, corrupt conduct and criminal activity involving Immigration and Border Protection Workers (ADD2016/1514516)
- *Public Governance, Performance and Accountability Act 2013*
- *Public Interest Disclosure Act 2013*
- *Public Service Act 1999*
- *Work Health and Safety Act 2011*

10. Consultation

10.1. Internal consultation

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

- Relevant policy and/or program management area:
 - Child Wellbeing Branch
 - Detention Assurance Branch
 - Detention Futures Operations
 - Detention Operations, including regional command
 - Onshore Contracts Section
- FOI, Privacy and Records Management Branch
- Integrity and Professional Standards Branch

For Official Use Only

- Legal Advice and Operational Support Branch
- Litigation Branch
- Media Operations Section
- Risk and Assurance Branch
- Strategic Advice Section (Secrecy and Disclosure Branch)
- Workforce Health and Safety Section

10.2. External consultation

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

- Serco Immigration Services

11. Document details

BCS Category/Function	Detention Management
BCS Sub-Category/Sub-Function	DM16 – Program Service Management
Period of Effect	31 July 2021

11.1. Document change 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 PCF requirements.
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.

11.2. Procedural Instruction approval

Document owner	Commander ABF Governance
Approval date	31 July 2018



Australian
BORDER FORCE

OPERATIONAL NOTIFICATION

Operational Notification Number: ON2018 - 36

To: Detention Network

Subject: Further instructions following the decision in the Full Federal Court on access to mobile phones in immigration detention

Effective Date: Immediately

Situation:

On Friday 22 June 2018, the Full Federal Court handed down their judgment in the matter of *ARJ17* regarding mobile phones in immigration detention. The Court found that the "blanket policy" of detainees not being permitted to possess mobile phones and SIM cards within immigration detention facilities, and that any such items found in their possession be confiscated until they leave the facility, was invalid.

On receipt of this judgment, instructions were issued to permit detainees in the detention network to possess their personal mobile phone(s).

The Department of Home Affairs (Home Affairs) decided not to make an application for special leave to appeal the matter to the High Court.

Advice / Action Required:

s. 42(1)

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

s. 42(1)



Any concerns or questions in regards to the information subject of this Operational Notification should be directed to the contact officer below:

Inspector, s. 22(1)(a)(ii), Detention and Removals Operational Policy, ABF Governance Branch


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

Email s. 22(1)(a)(ii)@abf.gov.au or s. 47E(d)@abf.gov.au

Approval:

Approved for distribution on 02 / 10 / 2018 by:

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



A/g Superintendent Planning & Engagement
ABF Governance I Strategic Border Command



Australian
BORDER FORCE

OPERATIONAL NOTIFICATION

Operational Notification Number: ON2019 - 12

To: All Regional Commands, Detention and Offshore Operations Command, Services Management and those involved in the operation of immigration detention facilities or for situational awareness.

Subject: Access to 'Smartwatches' and Activity Trackers in Immigration Detention Facilities

Effective Date: Immediately

Situation:

A smartwatch (such as an Apple Watch) is a wearable computer in the form of a wristwatch. Modern smartwatches provide a local touchscreen interface for daily use, while an associated smartphone app provides for management and telemetry (such as long-term biomonitoring). While early models could perform basic tasks, such as calculations, digital time telling, translations and game-playing, later model smartwatches have more general functionality closer to smartphones, including mobile apps, a mobile operating system and WiFi/Bluetooth connectivity.

Some smartwatches function as portable media players, with FM radio and playback of digital audio and video files via a Bluetooth headset. Some models, called 'watch phones' (or vice versa), have mobile cellular functionality like making calls.

An activity tracker, also known as a fitness tracker (such as FitBit and Garmin) is a wearable device or a computer application that records a person's daily physical activity, together with other data relating to their fitness, health, such as the number of calories burned, heart rate etc.

Advice / Action Required:

Activity Trackers

Activity trackers are considered to be a permitted item under detention policy. There are no restrictions placed on visitors, detainees or staff in immigration detention facilities (IDFs) possessing/wearing an activity tracker.

If a detainee requests their activity tracker from in-trust property, it must be made available to them. Further, there is no legislative authority to remove an activity tracker without consent from detainees except in the limited circumstances described below.

Smartwatches

Detainees:

Smartwatches are to be treated in the same way as mobile phones in IDFs.

If a detainee requests their smartwatch from in-trust property, it must be made available to

them. There is no legislative authority to remove a smartwatch without consent from detainees except in the limited circumstances described below.

In limited circumstances, officers may be able to remove a smartwatch from a detainee where, for example, it is reasonably necessary to keep the detainee in immigration detention or where there is a reasonably foreseeable risk of serious harm to the detainee.

If you are considering removing a Smartwatch (or an activity tracker) from a detainee, you should consult with Detention and Removal Operational Policy Section prior to any action being taken.

Visitors:

Visitors must continue to comply with the 'IDF Conditions of Entry' and are not permitted to bring mobile phones and smartwatches into the facility. If a visitor is in possession of a smartwatch, they must declare this to staff and store their smartwatch prior to their entry to the visitor area.

Unless an exemption is given by the ABF Detention Superintendent on a case-by-case basis, visitors will not be granted entry to the facility while in possession of a smartwatch.

Staff:

Departmental, ABF and contracted service provider staff in possession of a smartwatch must not enter the IDF (unless an exemption is given by the ABF Detention Superintendent on a case-by-case basis) in line with detention policy regarding controlled items.

Please note operational policy relating to other controlled items, including other internet enabled devices, such as computers with modems and iPads remains unchanged at this time. As such, this advice applies to Smartwatches and activity trackers only.

Related Policy and Procedural documents:

N/A

Any concerns or questions in regards to the information subject of this Operational Notification should be directed to the contact officer below:

Detention Policy Helpdesk
Email: s. 47E(d) [redacted]@abf.gov.au

Approval:

Approved for distribution on 05/04/2019 by
s. 22(1)(a)(iii) [redacted]

Superintendent Planning & Engagement
ABF Governance I Strategic Border Command



Australian
BORDER FORCE

OPERATIONAL NOTIFICATION

Operational Notification Number: ON2019 - 22

To: All Regional Commands

Subject: Control of items in immigration detention facilities

Effective Date: Immediately

Situation:

To ensure awareness and consistency across all Immigration Detention Facilities (IDFs), staff are reminded of what constitutes permitted and controlled items. To reiterate recent Federal Court decisions, mobile phones are now considered to be a permitted item within IDFs.

Advice / Action Required:

All staff are required to apply a consistent approach in line with the information provided in this Operational Notification when exercising discretion over what items detainees can possess in IDFs.

Permitted items: *Items permitted in all IDFs are those that are not detrimental to a detainee's health and the good order and security of the facility.*

Controlled items: *Items that are generally lawful under Australian law but have been deemed to present a risk to the health, privacy, safety, security and/or good order of the facility are permitted under specified conditions.*

Detailed information:

The following items are considered to be 'permitted' items:

- mobile phones
- energy drinks (subject to it being commercially packaged and labelled, factory sealed, displaying a visible and valid expiry date and not contained in any metal or glass packaging)
- noodles containing oil sachets (e.g. Mi Goreng noodles) (subject to it being commercially packaged and labelled, factory sealed, displaying a visible and valid expiry date and not contained in any metal or glass packaging)
- Easter eggs (subject to being commercially packaged, unopened and have a current expiry/best before date) – no requirement to remove foil
- batteries (e.g. AA, AAA)
- battery operated shavers/hair clippers (including beard trimmers)
- battery operated children's toys

- mobile phone chargers, including items that are for all practical purposes are a mobile phone charger, including power banks and wireless mobile phone chargers
- smart watches, and
- personal computers **without** a modem (APODs only).

If there is a concern about a detainee having possession of any items listed above or concerns about the entry of a possession to the IDF, the matter must be escalated to the relevant ABF Detention Superintendent (or delegate) for a review/decision.

The following items are considered to be 'controlled' items:

- electrical items for detainee use, subject to prior approval, space and safety considerations, and a current electrician's certificate stating compliance with relevant safety regulations, including:
 - Electric shavers/hair clippers (including beard trimmers)
 - Google Chromecast
 - PlayStation (or other personal gaming consoles), and
 - TVs.

ABF Detention Superintendents have the authority to approve a detainee's possession of controlled items and permitted items on a case-by-case basis. However, Superintendents must consult with Detention Operations National, before approving such request. A list of current identified Controlled Items is available at (ADD2019/4226580).

Operational policy relating to other controlled items, including internet enabled devices (other than mobile phones) such as computers with modems and iPads remain unchanged at this time.

Related Policy and Procedural documents:

- ON2018 – 36 – *Further Instructions following the decision in the Full Federal Court on access to mobile phones in immigration detention* (ADD2016-1361500)

Any concerns or questions in regards to the information subject of this Operational Notification should be directed to the contact officer below:

s. 22(1)(a)(ii) Superintendent Detention and Removal Operational Policy

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

Email: s. 22(1)(a)(ii)@abf.gov.au

Content authorised by:

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

Approved for distribution:

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

A/g Superintendent Planning & Engagement
ABF Governance I Strategic Border Command
23/07/2019



Rights and Responsibilities in Immigration Detention

Please take the time to read this carefully. By signing this document you confirm that you understand your rights and agree to comply with the responsibilities.

Your rights

- You will be treated with respect, dignity and courtesy
- Your information will be managed in accordance with Australian law.
- You have the right to reasonable access to communication, via telephone, mail, fax or email with your legal adviser(s), family members, subject to legal restrictions such as current Court Orders or Bail Conditions
- You will have access to materials and facilities for exercise, recreation, cultural expression, intellectual and educational pursuits
- You are free to profess and practice the religion of your choice, subject to Australian law and the good order and security of the facility
- You will be able to celebrate all major religious observances and festivals
- You will be able to receive visits from members of your family, friends, religious leaders, and approved members in the community, within the facility visiting hours, subject to visitor agreement to terms and conditions for entry into an immigration detention facility
- You have the right to be provided with access to translator services and interpreters
- You can receive visits from diplomatic, consular and legal representatives, the Australian Human Rights Commission, Commonwealth Ombudsman and the Australian Red Cross, unless there is a valid reason for the visit to be refused
- You have the right to refuse external visits
- You will be provided with sufficient food which is well-prepared and served
- You will be provided with access to medical and counselling services
- You will be provided with clean bed linen and toiletries for personal hygiene
- You have the right to comment or make complaints to the management of the facility regarding the conditions of, and your treatment, in immigration detention
- You have the right to make a complaint to external authorities including the Commonwealth Ombudsman and the Australian Human Rights Commission
- You have the right to request a meeting with your Status Resolution Officer
- If you want to contact police or other authorities, you will be able to access facilities to make a report. Any allegations of criminal activity occurring in immigration detention including allegations involving departmental, Serco and IHMS staff will be dealt with in accordance with Australian law
- You have the right to request access to your property held 'in trust'.

Your responsibilities

- You must not attempt to escape from immigration detention. It is an offence under the *Migration Act (1958)* to escape detention and it carries the possibility of a maximum of five years imprisonment
- A conviction for escaping detention may impact on your immigration status
- You must not discriminate, intimidate or bully any person, including departmental, Serco and IHMS staff
- You must not threaten, assault, or harass another person, including departmental, Serco and IHMS staff
- You must not initiate, conduct or participate in actions that are violent and can cause harm to others or can damage the facility's property
- You must not enter another person's personal space unless you are invited to. If the invitation is withdrawn you will have to leave that person's personal space immediately
- You are responsible for the care of your own belongings taken into the facility. The Department and Serco may not be liable for property lost while in your possession
- You must respect the right of others detainees and staff to privacy and confidentiality

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



- You must treat other detainees and staff in a respectful manner
- You must communicate your needs with courtesy and respect
- You are responsible for seeking clarification of any information when you don't understand it
- You are responsible for keeping your clothing and personal space clean and tidy
- If you bring medication into the facility, a qualified medical officer will decide how this medication will be managed and it is expected that you will use that medication according to the medical officer's instructions
- You are not allowed to possess any prohibited, excluded or controlled item
- You must not take property from others
- You must not hoard food, or take food from others
- You must not aid and abet others in committing an offence or discriminate against other persons including departmental and Serco staff
- You must respect other detainees right of access to shared facilities, including multi-faith areas
- You must comply with all reasonable orders and directions that are in the interest of the security and good order of this facility and the safety of all other persons including departmental and Serco staff, including but not limited to screening and searching of your person and property
- You must comply quickly and fully with the directions of departmental or Serco staff during an emergency
- You must comply with any change in room allocations as directed by staff
- You may be filmed by CCTV fixed cameras, staff hand-held cameras or body cameras worn by staff in order to ensure the security and good order of the facility and the safety of other persons including departmental, Serco and IHMS staff.

Failure to comply with these responsibilities

Failure to comply with the responsibilities set above can result in the following actions being taken against you:

- You may be moved to another part of the facility
- You may have your movements in the facility restricted
- You may be considered for transfer to another facility in the immigration detention network
- A Behavioural Management Plan about you may be developed and implemented
- May impact your immigration outcome

Failure to comply with the responsibilities may also affect your immigration outcome if the failure constitutes criminal activity that you are charged with, prosecuted, and convicted of, under the Australian law.

If you act against any Australian law or if you support and initiate activities that are against any Australian law, you may be charged and prosecuted in accordance with relevant state, territory or Commonwealth law, and you may be transferred to a correctional facility.



Terms and Conditions of Computer and Internet Use

Your access to the Department's Information and Computer Technology (ICT) services is conditional upon you agreeing to the terms and conditions of computer and internet use.

Your ICT activity will be logged and monitored for the purpose of preventing misuse and maintaining the integrity of the departmental ICT resources. You consent to the use by the Department of information concerning your ICT activity where the Department considers that information relevant for the purpose of undertaking official enquiries and investigations against you or another person.

Users under the age of 18 years will require consent from a parent or legal guardian to be given access to computers and the internet.

When using computer and internet services in immigration detention, you must:

- Use the booking system to book your preferred time for accessing a computer
- Comply with the terms and conditions of use of internet and computer as set out in this document
- Log on to the computer only with your allocated username and password*
- Log off the computer after you have finished your internet session*
- Respect the privacy of other computer users
- Use equipment in a way that maintains the good order and security of the facility and the safety and welfare of all people within it, including departmental and Serco staff
- Be responsible for disclosing your personal information over the internet
- Use the internet and network in a manner that is ethical, lawful and not to the detriment of others
- Report as soon as practicable any computer problems to the attending Serco officer
- Report any suspected compromise of your log-in or password to the Serco officer*
- Report any breach of this agreement by yourself or others to the Serco officer without delay.

Acceptable use

At the time you are issued with your allocated username and password, a Serco issued USB storage device may also be provided to you as required.*

While using the computer and accessing the internet you may:

- View web pages that do not breach these terms and conditions
- Use the Serco issued USB storage device to download and save files that are relevant to your immigration status, including any review process
- Attach files to outgoing emails that are relevant to your immigration status, including any review process
- Print up to 30 pages per day. This limit can be increased if there is a reasonable need by placing a request with the Serco officer.

Unacceptable use

- Do not use another person's username and password, or share your username and password with others. Every user will be held personally responsible for any and all activity conducted through their computer account*
- Do not bring food or drinks, or smoke near the computers
- Do not engage in offensive, illegal or criminal activities that could cause harm or offence to others
- Do not make an unauthorised reproduction of material protected by copyright
- Do not send or display offensive sites, videos or pictures that promotes or incites the commission of offences



- violence and sites using frequent, highlighted offensive language and sites relating to weapons
- Do not use the internet for commercial purposes
- Do not gamble or access dating/match-making sites
- Do not access child pornography
- Do not use software to download content from websites
- Do not exceed your allocated booking time for accessing a computer
- Do not engage in any activity that may cause damage to the computer hardware or software
- Do not attempt to repair or modify any of the computer hardware or software
- Do not create or post to personal blogs
- Do not create personal webpages, or group Facebook pages
- Do not access websites that contain or relate to:
 - Software downloads
 - Online storage
 - Any other inappropriate sites as they are identified.

Failure to comply with the terms and conditions

Failure to comply with the terms and conditions of computer and internet use in this document may affect your immigration outcome if the failure constitutes criminal activity under Australian law of which you are convicted or otherwise leads the Minister to conclude that you may not be a person of good character.

The following actions may be taken against you:

- A warning may be issued to you; and/or
- Your access to departmental ICT resources, including computer and/or internet resources, may be suspended or reduced, or subject to direct supervision by a departmental officer; and/or
- An investigation may be commenced in relation to your online activity.

While the Department respects your privacy and permits you to use this service as freely as possible, you acknowledge that the Department may monitor your use of the internet service. If the Department considers that your use of the Department's ICT equipment is, or may be, connected with criminal offending against an Australian law the Department **will** disclose relevant information collected as a result of any monitoring of your ICT use to relevant agencies responsible for investigating and prosecuting that offending.

Disclaimer

You are cautioned that the Internet may contain contents that are offensive, sexually explicit, and materials that may be deemed inappropriate. In general, it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content.

The Department and Serco make no warranty that the Internet or that any information, software, or other material accessible on the Internet is free of viruses, worms, Trojan horses or other harmful components which may corrupt or damage your files. By connecting, you acknowledge and accept the risks associated with access to the Internet.

The Department and Serco (and its representatives, agents or contractors) are not responsible for the content of any material prepared, received or transmitted by you.

Under no circumstances is the Department or Serco (and its representatives, agents or contractors) liable for any direct, indirect, incidental, special, punitive or consequential damages that result in any way from your use of or inability to use the computer facilities or to access the Internet or any part thereof, or your reliance on or use of information, services or merchandise provided on or through the Internet, or that result from mistakes, omissions, interruptions, deletion of files, errors, defects, delays in operation, or transmission, or any failure of performance.

A condition of using the facility's computer and internet resources, you agree not to violate any Commonwealth or State civil or criminal laws or breach any of these terms and conditions.



You agree to indemnify, exonerate, protect and hold harmless the Department and Serco (and its representatives, agents or contractors) from any claim, liability, loss, damage, cost or expense (including without limitation reasonable legal fees) arising out of or related to your use of the facility's computer and internet resources, any materials downloaded or uploaded through the use of those resources, any violation of any third party's rights or an violation of law or regulation or any breach of these terms and conditions.

Your personal information will be treated confidentially and only be used or disclosed in accordance with the provisions of the *Migration Act 1958*, the *Privacy Act 1988* or as otherwise required or authorised by law. Important information about the collection, use and disclosure of your personal and sensitive information (as defined in the *Privacy Act 1988*), including disclosure to other agencies, third parties, and overseas entities, is contained in the Department's Privacy Notice (Form 1442i). Copies of the Privacy Notice are available at www.border.gov.au, at any departmental office or Immigration detention facility. You can view the Department's Privacy Notice by clicking [here](#). You should ensure that you read and understand the Privacy Notice before agreeing.'

I understand and agree to the terms and conditions of computer and internet use. I consent to the collection, use and disclosure of my personal information for the purposes described above.

Note: Information marked with an asterisk (*) does not apply to you if you are accommodated in Christmas Island Immigration Detention Centre.

You will be asked to confirm that you have read and agree to adhere to the terms of this document. Please take time to read this carefully.

Serco Australia Pty Limited (**Serco**) and its related companies (**we, our, us**) are committed to complying with the Australian Privacy Principles contained in the *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* amending the *Privacy Act 1988 (Cth)* (**Privacy Act**). The Privacy Act requires us to notify an individual of certain matters when we collect personal information about them. This notice is your notification of those matters.

Serco is contracted to the Commonwealth of Australia to operate and manage immigration detention facilities around Australia. This statement explains how we collect and handle your personal information in relation to the services that we perform for the ABF, and should be read together with our Privacy Policy at <http://www.serco-ap.com.au/privacy-policy/>. Our Privacy Policy contains information about how you may access and/or seek correction of your personal information as well as information about how you may complain about a breach of the Australian Privacy Principles.

What is personal information?

The Privacy Act provides that personal information (including sensitive information) is information or an opinion about an individual who is reasonably identifiable. Sensitive information is a type of personal information and includes information about an individual's:

- health (including predictive genetic information)
- racial or ethnic origin
- political opinions
- membership of a political association, professional or trade association or trade union
- religious beliefs or affiliations
- philosophical beliefs
- sexual orientation or practices
- criminal record
- biometric information that is to be used for certain purposes
- biometric templates.

From whom Serco will collect your personal information

Serco collects personal information directly from you (as may be authorised by the ABF), the ABF, law enforcement agencies and correctional facilities or health services providers contracted by ABF to manage any medical conditions.

What are the main purposes of collection of your personal information?

Serco collects your personal information for the main purpose of performing services for the ABF as a contracted service provider under its contract to operate immigration detention services throughout Australia, including maintaining the safety and security of a person's time in detention.

Collection of your personal information that is required or authorised by law

The main pieces of legislation administered by the ABF are the *Migration Act 1958* (**the Migration Act**) and the *Australian Citizenship Act 2007* (**the Citizenship Act**). These Acts include specific provisions about the collection, use, and disclosure of your information. An example of where a law or order may require or authorise collection of sensitive information is the collection by an authorised officer under the Migration Act of personal identifiers (that may include biometric information) from a non-citizen who is in immigration detention.

The Privacy Act permits collection of sensitive information where it is authorised under law, or for enforcement related functions of the ABF, or with your consent other personal information where it is reasonably necessary for, or directly related to, one or more of ABF's functions or activities.

To whom will Serco disclose your personal information?

Serco is required to disclose your personal information to the ABF. Serco may also be required to disclose your personal information to other organisations to conduct enforcement activities as authorised by the ABF. Usual disclosures include as follows.

- Law enforcement agencies
- State and territory welfare agencies in relation to detention arrangements, care for unaccompanied minors or guardianship for detainees with physical and mental health disabilities
- Correctional facilities or other institutions where a detainee is transferred from our care to a prison, mental health facility or a hospital
- Government bodies or other agencies conducting inquiries and investigations, including an Ombudsman, the Australian Human Rights Commission or Privacy Commissioner)
- Organisations and agencies as may be required by other legislation or court orders

Complaints

If you believe your personal information is not properly protected, or that there has been a breach or potential breach of this Privacy Policy or the privacy legislation, please contact Serco immediately and ask for your complaint or concern to be directed to the Privacy Officer.

Serco takes breaches seriously and has procedures to help identify and resolve a breach, potential breach or complaint as quickly as possible. This includes appropriate escalation processes to the General Counsel and notification processes in the event of a breach. Every complaint is forwarded by the staff member who receives it to the Privacy Officer. You will be notified of the process for dealing with the breach or potential breach. Your complaint will be thoroughly investigated and a suitable resolution negotiated with you. If you are not satisfied with the resolution of your complaint by Serco, in Australia you may contact the Office of the Australian Information Commissioner (<http://www.privacy.gov.au/complaints>) who may investigate your complaint.

For enquiries or feedback about this policy or for complaints about Serco's handling of personal information, please email the Privacy Officer at privacy@serco-ap.com.au or otherwise you can mail to:

Privacy Officer
Serco Group Pty Ltd
Level 23, 60 Margaret Street, Sydney NSW 2000
Telephone: +61 (0)2 9964 9733

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

Family name		Given name	
Service ID		Reception type	
Arrival date		Document language	
	I agree to adhere to the terms of this document, as shown by my signature below	I do not agree to adhere to the terms of this document, as shown by my signature below	
Detainee rights and responsibilities	Agree	Disagree	
Internet and computer conditions of use	Agree	Disagree	
Privacy notice	Agree	Disagree	
I have received a copy of all documents		Yes	
I have received a facility induction briefing		Yes	
Signed			
Refused to sign		Date	
TIS#/Interpreter		Date	

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