



Home Office

Detention Services Order 05/2018

Mobile phones, internet enabled devices,
and cameras

June 2026



© Crown copyright 2024

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3 or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gov.uk.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at www.gov.uk/government/collections/detention-service-orders

Any enquiries regarding this publication should be sent to us at DSOConsultation@homeoffice.gov.uk

Contents

Contents	3
Document Details	5
Contains Mandatory Instructions	5
Introduction	6
Procedures	7
Possession of mobile phones, internet enabled devices and cameras	7
Detained individuals under escort	8
Detained individuals in a centre	9
Legal advisers	12
Official visitors	12
Social visitors	12
Contracted service provider staff	13
Home Office staff	13
Independent Monitoring Board members	13
HM Inspectorate of Prisons (HMIP) inspectors	14
Visiting medical professionals	14
Self-Audit	15
Revision History	16

Document Details

Process: To set out Home Office policy on mobile phones, internet enabled devices and cameras in immigration removal centres, residential short-term holding facilities, the pre-departure accommodation and during escort.

Publication Date: June 2026

Implementation Date: December 2018 (reissued June 2026)

Review Date: June 2028

Version: 4.0

Contains Mandatory Instructions

For Action: All Home Office staff and contracted service providers operating in immigration removal centres (IRCs), short-term holding facilities (STHFs), pre-departure accommodation (PDA) and charter or scheduled flights.

Author and Unit: Dean Foulkes, Detention Services.

Owner: Michelle Smith, Head of Detention Operations.

Contact Point: [Detention Services Orders Team](#).

Processes Affected: All processes relating to the possession of mobile phones, internet enabled devices and cameras.

Assumptions: All staff will have the necessary knowledge to follow these procedures.

Notes: N/A

Introduction

1. This Detention Services Order (DSO) sets out Home Office policy on the possession of mobile phones, internet enabled devices and cameras by detained individuals, staff, visitors, legal advisers and visiting healthcare professionals in immigration removal centres (IRCs), residential short-term holding facilities (RSTHFs), pre-departure accommodation (PDA) and charter or scheduled flights.
2. This instruction **does not** apply to those detained in a non-residential STHF or Residential Holding Rooms (RHRs); instead local procedures apply in line with the [Short-term Holding Facility Rules 2018](#).
3. For this DSO:
 - 'centre' refers to IRCs, RSTHFs and PDA.
 - 'Centre manager(s)' refers to the contracted immigration removal centre/short-term holding facility manager (i.e., it does not refer to on-site Home Office staff).
 - 'Service provider' includes all suppliers operating in centres, as defined above, and escort providers.
 - 'Internet enabled devices' refers to any device capable of accessing services through a mobile or other wireless network. This includes handheld mobile devices, smartphones or feature phones, tablets, smart watches, e-readers, portable games consoles, etc.
4. Two different Home Office teams operate in IRCs:
 - Detention Services Compliance team (Compliance team)
 - Immigration Enforcement Detention Engagement team (DET)

The **Compliance team** is responsible for all on-site commercial and contract monitoring work. The **DETs** interact with detained individuals face-to-face on behalf of responsible officers within the IRCs. They focus on communicating and engaging with people detained at IRCs, helping them to understand their cases and detention.

There are no DETs at the Gatwick PDA or RSTHFs. The functions which are the responsibility of the DET in IRCs, are instead carried out by the contracted service provider in RSTHFs and overseen by the International and Returns Services (IRS) Escorting Contract Monitoring Team (ECMT). In the Gatwick PDA, the role of detention engagement is covered by the local Compliance Team.

Procedures

Possession of mobile phones, internet enabled devices and cameras

5. Below is a simple summary of who may have mobile phones, internet enabled devices or cameras in a centre and the type of phone they may have:

Group	Are allowed
Detained individuals	<p>One of the following:</p> <ul style="list-style-type: none"> - access to their own personal mobile phone without a camera, recording and internet facilities (subject to restrictions explained later in this instruction); - a mobile phone issued by the centre that has no access to a camera, recording and internet facilities. - a mobile phone issued by the centre that has no access to a camera function but has limited internet functions. The centre can only operate these mobile phones through a secure wireless network approved by the Home Office.
Legal advisers	<ul style="list-style-type: none"> - access to a mobile phone (or camera) with recording/internet facilities in designated visits areas.
Official visitors	<ul style="list-style-type: none"> - access to a mobile phone, camera or internet enabled device with recording/internet facilities in areas not frequented by detained individuals. - access to a mobile phone without recording/internet facilities in areas frequented by detained individuals.
Social visitors	<ul style="list-style-type: none"> - no access to a mobile phone, internet enabled device or camera of any sort within any part of the centre.
Contracted service provider staff	<ul style="list-style-type: none"> - no access to a mobile phone, internet enabled device or camera of any sort within any part of the centre without authorisation by the centre manager.
Home Office staff	<ul style="list-style-type: none"> - access to a mobile phone or internet enabled device with recording/internet facilities in areas not frequented by detained individuals. - access to a mobile phone without recording/internet facilities in areas frequented by detained individuals. - with the permission of the centre manager, access to a mobile phone (or camera) with recording facilities or internet enabled device in areas frequented by detained individuals.

Group	Are allowed
Home Office auditors, security team or other Home Office staff attending centres on pre-arranged official visits	- To take a camera, without access to the internet, into the establishment if necessary for monitoring or audit purposes and were authorised by the centre manager. See paragraph 38,
IMB Members	- Retain their mobile telephones whilst visiting an IRC or STHF unless the Centre Manager is aware of exceptional and identifiable safety or security reasons that require a modification of such practice. - All mobile phones held by IMB members should be declared at the entrance to the centre and are liable for inspection both on arrival and on departure.
HM Inspectorate of Prisons' staff	- access to a mobile phone or internet enabled device with recording/internet facilities in areas not frequented by detained individuals. - access to a mobile phone without recording/internet facilities in areas frequented by detained individuals. - to take a camera, without access to the internet, into the establishment.
Visiting Medical Professionals	- access to a mobile phone which takes photos but without internet access in consultation areas. - access to a camera, without access to the internet, in consultation areas if that is their preference for taking photos. - access to a mobile phone which does not take photos and without recording/internet facilities in areas with free access for detained individuals.

Detained individuals under escort

6. Whilst under escort for the purposes of removal, detained individuals are allowed to have a mobile phone in their possession if it is without:
- recording facilities, i.e., the ability to take photographs, video, live-streaming or audio recording; and
 - facilities to connect to the internet.
7. Detained individuals must be allowed to keep their personal mobile phone if it complies with these restrictions. However, following a risk assessment, provision of a mobile phone may be denied in the following circumstances:
- a) Current disruptive or threatening behaviour provides evidence that the individual may misuse the mobile phone; and/or

- b) There are specific risks to the public confirmed by a public protection arrangement such as multi-agency public protection arrangement (MAPPA); and/or
 - c) There are reasonable grounds to believe that the detained individual may use the mobile phone to cause harm to be done to themselves or another person.
8. If the detained individual's phone does not comply with the allowed requirements outlined in paragraph 5 and consequently has been removed from them, or it has been removed following a risk assessment, escort staff must ensure that this does not prevent the detained individual's access to justice by enabling them to access suitable alternative methods to speak to their legal representatives or to contact a court. Escort staff must explain to detained individuals how to contact legal representatives/a court by phone during escort.
9. Detained individuals who are being escorted for the purposes of transfer: a) between establishments; b) to bail or court hearings; c) to an embassy/high commission; or d) to outside medical appointments, are not allowed to have a mobile phone in their possession due to the risk to officer/public safety and detained individual security.
10. Detained individuals should be allowed to contact legal representatives/a court on request, providing it is safe and secure to do so. In the very rare circumstances where a detained individual is denied access to a phone for safety or security reasons, a written record of the request, detailing the reasons for refusal, must be made as an entry on the detained individual's Person Escort Record (PER). The escorting staff must also notify the Detention Estate Population Management Unit (DEPMU) of a refusal to allow such contact by completing form IS91RA Part C with the details and reasons for the refusal and the name of the officer authorising the refusal.
11. If a detained individual is deaf or has hearing difficulties which means that they cannot use a phone, members of staff must ensure that this does not impede/prevent the detained individual's access to justice, by providing more suitable, alternative methods to liaise with their legal representatives or to contact a court (e.g., via written communication/ensuring welfare officers can signpost them to the relevant information).

Detained individuals in a centre

12. Whilst held in a centre, detained individuals are allowed to have a mobile phone in their possession in line with one of the following criteria:
- a) access to their own personal mobile phone without a camera, recording and internet facilities.
 - b) a mobile phone issued by the centre that has no access to a camera, recording and internet facilities.

- c) a mobile phone issued by the centre that has no access to a camera function but has limited internet functions. The centre can only operate these mobile phones through a secure wireless network approved by the Home Office.

13. Following a risk assessment by the contracted service provider, provision of a mobile phone in the following circumstances may be denied:

- a) Current disruptive or threatening behaviour provides reasonable grounds to believe that the detained individual will misuse the mobile phone; and/or
- b) There are specific risks to the public confirmed by a public protection arrangement such as MAPPA; and/or
- c) There are reasonable grounds to believe that the detained individual will use the mobile phone to cause harm to be done to him or herself or another person.

14. Any denials of the provision of a mobile phone must be recorded, and the Compliance Manager notified (HEO or above). Any denial exceeding a period of 1 week must be authorised by the Compliance Manager and reviewed on a weekly basis. The detained individual can appeal any decision to deny the provision of a mobile phone, providing reasons in writing to the contracted service provider Centre/Deputy Manager, who will decide within 48 hours.

15. Where a detained individual is not allowed a mobile phone in accordance with paragraph 13, members of staff must ensure that this does not prevent the detained individual's access to justice by enabling access to suitable alternative methods to speak to their legal representatives or to contact a court. Their mobile phone must be stored securely for the time they are not permitted to retain one.

16. Detained individuals must have the option to keep their personal mobile phone if it complies with the restrictions at paragraph 12a and subject to the risk assessment in paragraph 13. When personal mobile phones do not comply with such restrictions, they must be stored securely with any other internet enabled devices or cameras in the detained individual's property so long as the individual remains in detention.

17. Subject to the risk assessment detailed in paragraph 13, centres must provide appropriate mobile phone handsets to all detained individuals that do not own a mobile phone or whose personal mobile phone does not comply with the restrictions of paragraph 12a.

18. When needed, detained individuals must be given assistance with transferring stored phone numbers to the mobile phone provided by the centre or to make a note of the required contacts. Where the technology allows, detained individuals should be allowed to keep their own phone number. Detained individuals should also be given the

opportunity to divert their personal mobile phone to the new handset provided by the centre and to leave a voicemail message informing callers of their temporary number.

19. Mobile phones must be provided free of charge to the detained individual. However, if the detained individual repeatedly (i.e., on more than two occasions) damages or loses the mobile phone, the IRC contracted service provider can apply a nominal fee for the replacement of the mobile phone. This fee should be agreed with the local Compliance Team Manager and be explained to the detained individual when issuing the handset.
20. All detained individuals are entitled to a five-minute free call when they first arrive at a centre. A five-minute free call must also be provided following inter-centre transfers.
21. Detained individuals should, where possible, be able to retain their own SIM card. If they do not have a SIM card, or their SIM card is not compatible with the device provided, centres are required to provide one where a SIM enabled device is being used. Detained individuals must be able to choose their mobile phone service provider or where SIM enabled devices are not available, use the centre's secure wireless network phones.
22. A variety of SIM cards and pre-pay/top-up cards should also be sold in the centre shop. It is the detained individual's decision which mobile phone operator they choose for SIM enabled devices. Detained individuals should be made aware of any signal coverage issues which might affect their choice.
23. Contracted service provider centre managers are responsible for ensuring a record is kept of all mobile phones in the possession of detained individuals, including:
 - a) the name of the detained individual.
 - b) IMEI number; and
 - c) a record of the phone numbers issued, if any.
24. This record must be kept for all mobile phones and SIM cards in the possession of detained individuals whether received at reception, through the post, following a visit or purchased from the shop.
25. When a detained individual is found to have three or more SIM cards in possession, this should be investigated by the centre's security team. In accordance with [DSO 11/2014 Security Information Reports](#), a Security Information Report must be completed with the details of this find and sent to the local Compliance Team Manager and the Detention Services Security Team.
26. If a detained individual is deaf or has hearing difficulties which mean that they cannot use a phone, members of staff must ensure that this does not prevent the detained individual's access to justice by enabling access to suitable alternative methods to communicate with their legal representatives or to contact a court.

Legal advisers

27. Rule 2 of the Detention Centre Rules 2001 (SI 238/2001) defines 'legal advisers' in relation to a detained person as his/her "counsel, representative or solicitor, and includes a clerk acting on behalf of his/her solicitor". 'Legal adviser' is defined in the Short-term Holding Facility Rules 2018 as "a detained person's counsel, representative or solicitor, and includes a clerk acting on behalf of that solicitor;"
- Please note that the Detention Centre Rules 2001 and Short-term Holding Facility Rules 2018 do not apply to the Pre-Departure Accommodation, but this definition is nevertheless also assumed to apply in relation to these types of detention facility.
28. Legal advisers may retain their mobile phone when visiting a detained individual in a designated visits area.
29. All mobile phones or internet enabled devices held by legal advisers must be declared at the entrance to the centre and are liable for inspection both on arrival and on departure. Any failure to disclose a mobile phone when entering a centre must be investigated and recorded by the centre's security department and referred to the Detention Services Security Team. Such breaches of security must be considered on an individual basis and, where appropriate, may result in a referral being made to the Home Office Director of Detention Services for the banning of the visitor, in accordance with [DSO 04/2012 Visits and Visitors](#).

Official visitors

30. Official visitors are those persons whose visits are being hosted by the centre manager or by any Home Office member of staff.
31. Official visitors may retain their personal mobile phone during their visit when they are in areas not frequented by detained individuals.
32. Personal mobile phones or internet enabled devices with recording and internet facilities may not be brought into areas frequented by detained individuals, unless the visitor has the permission of the contracted service provider centre manager to do so.
33. All mobile phones and internet enabled devices held by official visitors must be declared at the entrance to the centre and are liable for inspection both on arrival and on departure.

Social visitors

34. Social visitors are not permitted to bring a mobile phone into any centre under any circumstances. Visitors may deposit phones, internet enabled devices or cameras in

lockers outside the centre (where provided) for the duration of their visit, but this is at their own risk.

35. Visitors can be liable for inspection in accordance with the centre's normal searching policy (as per [DSO 09/2012 Searching Policy](#)) and may be banned if found to be caught in possession of a prohibited item, including a phone, during a search.
36. A social visitor may hold a pager but is also liable for inspection in accordance with the centre's normal searching policy.

Contracted service provider staff

37. Service provider staff access to a mobile phone is at the discretion of the centre manager. Service provider staff should have no access to a mobile phone, of any sort, within any part of the centre without authorisation by the centre manager.
38. All mobile phones and internet enabled devices held by service provider staff should be declared at the entrance to the centre and are liable for inspection both on arrival and on departure.
39. Service provider staff must follow their organisation's security guidance.

Home Office staff

40. Any Home Office staff may have access to a mobile phone or other internet enabled devices with recording facilities in areas not frequented by detained individuals and access to a mobile phone without recording/internet facilities in areas frequented by detained individuals.
41. All Home Office staff should declare all mobile phones and internet enabled devices in their possession on entrance to the centre, if requested. Phones and internet enabled devices are liable for inspection both on arrival and departure.
42. Home Office auditors or security team staff attending a centre for official auditing purposes may arrange to take a camera, without internet access, into the centre to record their findings. This must be previously arranged and approved by the Centre Manager or their deputy. Gate staff must log and account for the camera and any memory card contained in it at the end of the audit and may request to inspect all photos taken, before authorising the camera to leave the centre.

Independent Monitoring Board members

43. Independent Monitoring Board (IMB) members shall retain their mobile telephones whilst visiting an IRC or STHF unless the Centre Manager is aware of exceptional and identifiable safety or security reasons that require a modification of such practice. All

mobile phones held by IMB members should be declared at the entrance to the centre and are liable for inspection both on arrival and on departure.

44. When monitoring a charter flight, IMB members can have access to their mobile phones or other internet enabled devices with recording facilities whilst travelling on coaches to the airport and during the flight to the destination country.
45. The recording functions (sound, photos and video) of such mobile phones or other internet enabled devices should not be activated without the prior permission of the escorting contracted service provider Senior Security Officer or the Home Office Chief Immigration Officer.
46. IMB members should not make their mobile phones or other internet enabled devices with recording facilities available to returnees without the prior permission of the escorting contracted service provider Senior Security Officer.

HM Inspectorate of Prisons (HMIP) inspectors

47. HMIP inspectors may take a camera into the centre. Gate staff must log and account for the camera when the inspector leaves the centre. All photos will be provided to Home Office Immigration Enforcement as part of the factual accuracy check of the draft inspection report. Therefore, gate staff should not ask to inspect the photos taken on the camera before the inspector leaves the centre.
48. When inspecting a charter flight, HMIP inspectors can have access to their mobile phones or other internet enabled devices with recording facilities whilst travelling on escorting contracted service provider coaches to the airport and during the flight to the destination country.
49. To minimise the risk of returnee disruption because of photos or videos being taken, the recording functions (sound, photos, and video) of such mobile phones or other internet enabled devices should not be activated without the prior permission of the escorting contracted service provider Senior Security Officer or the Home Office Chief Immigration Officer.
50. HMIP inspectors should not make their mobile phones or other internet enabled devices with recording facilities available to returnees without the prior permission of the escorting contracted service provider Senior Security Officer.

Visiting medical professionals

51. A visiting medical professional is a registered medical practitioner (a medically qualified doctor or dentist who is registered with the General Medical Council or General Dental Council) or a registered nurse who is appointed by the detained individual or their legal

representative to attend to them in accordance with Detention Centre Rules 33(7) or 33(11).

- Please note that the Detention Centre Rules 2001 do not apply to residential Short Term Holding Facilities or the Pre-Departure Accommodation, but this definition is nevertheless also assumed to apply in relation to these types of detention facility.

52. Visiting medical professionals may hold a camera without access to the internet or a mobile phone (or similar devices) with a facility to take photographs where it is required for collecting medical evidence. However, phones or internet enabled devices with an ability to connect to the internet, to provide streaming or audio recording will not be permitted. Visiting medical professionals may therefore prefer to bring a camera into the centre for the collection of medical evidence.

53. The medical professional should be informed that the mobile phone or camera may be used solely for the purpose of taking photographic medical evidence in relation to the detained individual being visited.

54. The medical professional should be instructed to always keep the phone or camera with them whilst in the centre and not to leave it unattended at any time.

55. Mobile phones, internet enabled devices and cameras held by visiting medical professionals must be declared at the entrance to the centre. A member of the healthcare team at the centre - rather than gate staff - should inspect the photos taken on the phone or camera before it leaves the centre. Gate staff must log and account for the phone or camera when the medical professional leaves the centre.

Self-Audit

56. An annual self-audit of this DSO is required by contracted service providers to ensure that the processes are being followed. This audit should be made available to the Home Office on request.

Revision History

Review date	Reviewed by	Review outcome	Next review
Jan 2017	Jose Domingos	Reformat	January 2019
December 2018	Shadia Ali	Amended to include the roll out of DET teams and individual responsibilities.	December 2020
April 2024	Dean Foulkes	Updated to reflect: <ul style="list-style-type: none"> • The addition of requirements when detained individuals are permitted to have a mobile phone in their possession. • Clarification on the use of mobile phones, internet enabled devices and cameras for IMB members. • That denials for provision are recorded, and were exceeding a period of 1 week, who is responsible for authorising this. 	April 2026
June 2026	A. Shourie	Self-audit requirements in relation to the Compliance Teams has been updated.	June 2028