Home Office

Detention Services Order 04/2016

Access to the internet within the Immigration Removal Estate

July 2024

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

Document Details

Process: To provide instructions and operational guidance for Home Office staff and contracted service providers on the provision of internet access for detained individuals.

Publication Date: July 2024 (reissued February 2026)

Implementation Date: May 2016 (reissued July 2024)

Review Date: July 2026

Version: 3.0

Contains Mandatory Instructions

For Action: All Home Office staff and contracted service providers operating in immigration removal centres, residential short-term holding facilities and pre-departure accommodation.

For Information: N/A (Whilst this DSO incorporates mandatory actions for Home Office responsible caseworkers, this guidance is for informational purposes only).

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 provision of internet access within the removal estate.

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

Notes: N/A

Instruction

Introduction

1. This Detention Services Order (DSO) provides instructions and operational guidance for all Home Office staff and contracted service providers operating in immigration removal centres (IRCs), pre-departure accommodation (PDA) and residential short-term holding facilities (RSTHFs).

2. For this guidance, 'centre' refers to IRCs, PDA and RSTHFs.

3. This instruction **does not** apply to Residential Holding Rooms (RHRs) or non-residential short-term holding facilities.

4. Two different Home Office teams operate in IRCs:

    - Detention Services Compliance team (Compliance team)
    - Detention Engagement team (DET)

The Compliance team are 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, serving paperwork on behalf of caseworkers and helping them to understand their cases and detention.

There are no DETs at RSTHFs, or the Gatwick PDA. Some of the functions which are the responsibility of the DET in IRCs, are instead conducted by the contracted service provider and overseen by the International and Returns Services (IRS) Escorting Contract Monitoring Team (ECMT) in RSTHFs. In the Gatwick PDA, the local Compliance Team cover the role of detained individual engagement.

Purpose

5. The purpose of this order is to ensure that detained individuals have reasonable and regulated access to the internet, whilst ensuring that the security of the immigration removal estate is not undermined.

Procedures

6. All detained individuals must have access to any non-prohibited category of website (see paragraph 13), such as education, legal and news websites, to assist with maintaining links with friends, families, and legal representatives and to prepare for

removal. DSO 07/2013 Welfare provision in Immigration Removal Centres sets out more general guidance for staff on welfare provision in IRCs.

Provision of Internet Facilities

7. Each centre should ensure that internet access enabled computer terminals are available to detained individuals 7 days a week for a minimum of 7 hours a day, though individual time slots may be limited if there is excessive demand or unforeseen service interruption (such as internet problems, see paragraph 22 for reporting incidents for loss of internet service).

8. Regulated access to the internet and any personal internet-based email accounts will be provided to detained individuals, subject to them signing up to the individual centre's acceptable use policy for internet use, using the form at Annex A of this DSO. Where it is determined that the detained individual has insufficient knowledge of English to understand the acceptable use policy, the policy should be read to the detained individual and explained in a language that they understand.

9. A decision to suspend internet access from a detained individual can be taken by the contracted service provider Centre/Deputy Centre Manager, for example for security or safety reasons or because a detained individual is in breach of the centre's acceptable use policy on the use of the internet. An application to suspend internet access must be supplied by the Security department to the Compliance Team for approval, and any subsequent decision must be recorded by contracted service provider staff, with the detained individual being notified in writing of the suspension and the reason for it. For those residents with an insufficient proficiency/knowledge of English, an interpreter on-site may be used to explain this in a language they understand. A decision to suspend should not be used as a sanction for wider non-compliance by a detained individual.

10. The Compliance Manager must be notified of any suspension and the reasons for it. Any suspension exceeding a period of 1 week must be authorised by the DS Compliance Manager (grade HEO or above) and reviewed on a weekly basis until suspension has ended. The detained individual can appeal any decision to suspend, providing reasons in writing to the contracted service provider Centre/Deputy Manager, who will decide within 48 hours. For detained individuals with a removal direction within 24 hours, the decision should be made within 12 hours.

11. If a detained individual has their access suspended and requires access to the internet for material relevant to their immigration case, the detained individual can approach the IRC's welfare office who will provide limited supervised access on a case-by-case basis.

12. Where the contracted service provider is notified by the Home Office/court that the detained individual has licence conditions regarding restrictions on accessing the internet, they must follow the procedure to request a permanent internet ban for the individual upon arrival. The contracted service provider must ensure the detained

individual is notified of the ban / restrictions in writing. For those residents with an insufficient proficiency/knowledge of English, an interpreter on-site may be used to explain this in a language they understand.

13. Contracted service providers should ensure that detained individuals are able to easily access any material on the internet that may be relevant to their immigration case if it does not fall within a prohibited category. This will include, but is not exhaustive to, Home Office rules and guidance; court and tribunal proceedings and judgments; information about access to legal representation and legal reference websites. In addition, access to the official websites of UN and EU bodies; foreign governments; non-governmental organisations, including those interested in immigration detention; UK and foreign newspapers; examination websites such as City and Guilds; and other education related websites should be provided.

14. Where a detained individual requires access to a site, that is likely to be prohibited, regarding their immigration case, they should approach the IRC welfare office to discuss access. (see DSO 07/2013 on the welfare provision in IRCS)

15. The contracted service provider must ensure that detained individuals are unable to access any website that falls within the list of prohibited categories, both English and foreign language sites, as follows:

    Prohibited lifestyle categories
    - Social media (including Facebook, Twitter, chat rooms and instant messaging)
    - Pornographic material
    - Dating
    - Gambling

    Prohibited security categories
    - AI such as ChatGPT or similar programs/apps
    - Use of VPNs (Virtual Private Networks) such as Proton VPN

    Prohibited harm related categories
    - Terrorism (extremist and radicalisation material)
    - Weapons and explosives
    - Racist material
    - Other crime

16. The contracted service provider should ensure that a list of any detained individuals attempting to view, send or receive information related to prohibited harm related categories, sites or keywords/phrases is recorded and shared with the Compliance manager on a weekly basis. Where there are serious/repeated incidents, such as attempts to access any extremist or radicalisation websites, the DS Compliance

manager (grade HEO or above) should be informed as soon as possible, and these websites will either subsequently be blocked, or the detained individual's internet access will be suspended as per Rule 29 (3) of Short-Term Holding Facility Rules 2018. For those residents with an insufficient proficiency/knowledge of English, an interpreter on-site may be used to explain this in a language they understand. A security information report (SIR) must also be completed by the contracted service provider in addition to a counterterrorism (CT) referral where appropriate, as set out in DSO 11/2014 Security Information Reports, and uploaded to the Intelligence Management System (IMS) in line with DSO 01/2015 Extremism and radicalisation. A copy of the SIR and/or CT referral should be forwarded to the Detention Services Security Team inbox.

17. A summary of any internet or email breaches, for example, attempting access to any prohibited categories as in paragraph 16, should be submitted to the Compliance manager monthly.

Adding and Removing Access to Individual Websites

18. A detained individual can request access to a blocked website by making an application in writing to the contracted service provider manager responsible for internet provision. For those residents with an insufficient proficiency/knowledge of English to make an application, an interpreter on-site may be used to explain this in a language they understand. The contracted service provider will check the content of the website and, if it falls outside a prohibited category, the contracted service provider Centre/Deputy Centre Manager will arrange for the detained individual to have access within 48 hours (or as soon as possible for STHFs), unless there are exceptional circumstances where access is required more quickly, for example if documents are required for a detained asylum case interview/appeal.

19. The date and time of the request and when access was subsequently granted should be recorded by the contracted service provider. If a detained individual's request for access to a specific website is denied, the detained individual should be informed in writing of the decision by the contracted service provider Centre/Deputy Centre Manager, ensuring the detained individual understands what is written (i.e., if the website being denied is in relation to an ongoing claim) and the IRC Compliance team should be notified.

20. This monthly report must be sent to the relevant Compliance manager (HEO or above) by no later than the third day of the following month. There is an expectation that the Compliance team reviews the monthly report for accuracy before forwarding it to (inbox: DESManagementInformation@homeoffice.gov.uk) by no later than the 7th day of that same month. The combined log from all centres will then be sent to each centre's internet administrator. On receipt of the log, each contracted service provider should review their centre's internet provision and take action to ensure that detained individuals have access to all 'enabled' websites on the log and that all 'withdrawn' websites are blocked, within 3 days, logging the date and time that the request was

actioned. If a contracted service provider has a concern with either adding or removing a specific website, they should escalate to the Compliance Delivery Manager in the first instance.

Loss of Internet Service

21. In the event of a loss of internet service the incident reporting process should be followed as set out in DSO Reporting and communicating incidents.

Monitoring and Audit

22. The contracted service provider must ensure that the centre's network infrastructure is robust and secure and that effective security measures are in place to prevent unauthorised access by any device or detained individual.

23. Local procedures must be in place to ensure machines have anti-virus/malware software installed that is updated daily and cannot be disabled by the user. This must be monitored by the contracted service provider by conducting periodic testing to ensure security measures are in place on the authorized devices.

24. Additionally, the contracted service provider is responsible for the regular testing of these safeguards and must provide evidence that this is being monitored to the local Compliance and Security team. The centre's Local Security Strategy (LSS) should include a reference to IT and internet security.

25. Any electronic communications to or from a detained individual containing privileged material (such as legal correspondence) must be excluded from all monitoring.

26. The contracted service provider is responsible for monitoring in real time all active internet sessions in the room and be able to immediately curtail an internet session in case of a security or other breach, such as a deliberate attempt to access a prohibited website.

27. Following initial log on, detained individuals should not be able to swap terminals during their session and the contracted service provider must ensure that there is a clear audit trail in place to match detained individuals with terminals, for example using CCTV. All terminals must also be logged off or in a secure state at the end of a session and all terminals must be inspected at the end of each session to ensure that all terminals are secure, recording the check in the wing or area diary.

28. Downloading or uploading of any files by a detained individual is prohibited for security reasons. If a detained individual wishes to print a document or email attachment, the contracted service provider should ensure that there are effective processes in place to print a document or email attachment. Support should be provided from the welfare office for detained individuals wishing to print legal/medical information to ensure that the confidentiality of this material is maintained during printing. This should be actioned within 24 hours (or within 2 hours for STHFs), subject to approval by the contracted service provider's security manager.

Revision History

Review date	Reviewed by	Review outcome	Next review
January 2020	Shadia Ali	Amended to include- • the roll out of DET teams and individual responsibilities • Email address to send monthly log was updated • further guidance provided on network testing	January 2022
July 2024	Dean Foulkes	Updated to reflect: • Terminology changes from 'detainee' to detained individual, and 'centre supplier' to contracted service provider. • Contingency for loss of internet service	July 2026
February 2026	Akash Shourie	Minor amendment: • Paragraph 15 amended to add in 'Prohibited Security Categories', updating in line with and as requested by GDPR Lead with regards to the use of AI technology	July 2026

Annex A
Use of the internet – acceptable use policy

Use of the Internet

1. You can use the internet in this Centre, to help you to stay connected with your friends and family and to prepare for your removal from the United Kingdom.

2. Staff can provide you with help and advice on using the internet if you are not familiar with it already. IT courses are also available to help you further. Ask a member of staff for more details.

3. Internet use will always be monitored by contracted service provider staff when the room is in use.

4. Use of the following types of websites is prohibited:
   Prohibited lifestyle categories:
   - Social networking (including Facebook, Twitter, chat rooms and instant messaging)
   - Pornographic material
   - Dating
   - Gambling

   Prohibited security categories
   - AI such as ChatGPT or similar programs/apps
   - Use of VPNs (Virtual Private Networks) such as Proton VPN

   Prohibited harm related categories:
   - Terrorism (extremist and radicalisation material)
   - Weapons and explosives
   - Racist material
   - Other crime

5. Use of the internet is subject to a few terms and conditions, which are **summarised in this policy**. Detailed terms and conditions are also available in every internet suite. Any attempt to misuse the facilities or to breach the terms and conditions may lead to your access to the internet being suspended.

6. By signing this form, you are agreeing to adhere to the terms and conditions and acknowledge that your internet use will be monitored.

You should also note that any activity which is perceived to have contravened the law will be reported to the police and may lead to your prosecution.

Code of Conduct

You must:

- Be conscious of and respect other users, including their right to work in privacy and in a quiet environment.
- Always protect your log-in and password.
- Only attempt to connect to the internet using your own log-in and password.
- Log off completely when you leave the internet suite.
- Report any suspected compromise of your log-in or password to a member of staff.
- Report any breach of this policy by yourself or others to the contracted service provider without delay.

You must not:

- Share your log-in or password details with any other detained individual.
- Swap terminals with another user without logging off completely first and then re-connecting using your own log-in and password.
- Allow another detained individual to use a terminal which is already logged in using your details.
- Use the internet to engage in any unlawful activity.
- Deliberately access prohibited sites.
- Create, send or print any material which is unlawful or is likely to cause offence to others, including pornographic (of any description), racist, or homophobic material.
- Attempt to install any software onto a terminal.
- Attempt to download any commercial software or copy-righted materials, including music or videos for use on mobile telephones or other portable devices.
- Attempt to connect to any other network, regardless of whether it was authorised by the third party.
- Attempt to introduce any form of computer virus or spy-ware onto the network.
- Attempt to save any material on a portable device, including CDs, DVDs, memory sticks, mobile telephones or other such devices.

Agreement

I have read/I have had this read to me and I understand the contents of this policy concerning the use of the internet and agree to abide by its terms and conditions. I accept that my use of the internet will be monitored and recorded and that any breach of this policy may result in me being suspended from using the internet facilities. I also

understand that any attempt to engage in any unlawful activity will be reported to the police and may result in criminal prosecution.

Name	Signature	Date