Home Office

Detention Services Order 04/2016

Detainee Access to the Internet

Process**:** To provide instructions and guidance for staff and suppliers on the provision of internet access for detainees

Implementation Date: May 2016
Review Date: May 2018

Contains Mandatory Instructions

For Action: Home Office staff and suppliers operating in immigration removal centres, pre-departure accommodation and short-term holding facilities.

For Information: Home Office caseworkers

Author and Unit: Frances Hardy, Operational Support and Guidance

Owner: Alan Gibson, Head of Detention Operations

Contact Point: Frances Hardy

Processes Affected: Processes relating to the provision of internet access within the detention estate

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

Notes: There are no previous DSOs on this subject

Issued: May 2016
Version: 1.0

Detention Services Order 04/2016

Detainee Access to the Internet

Contents

Introduction

1. This order provides guidance for all staff in Home Office immigration removal centres (IRC), pre-departure accommodation (PDA) and residential short-term holding facilities (STHF). This excludes immigration detainees accommodated in prison.

Purpose

2. The purpose of this order is to ensure that detainees have reasonable and regulated access to the internet whilst ensuring that the security of the detention estate is not undermined.

Procedures

3. All detainees must have ready access to any non-prohibited category of website (see paragraph 8), 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 sets out more general guidance for staff on welfare provision in IRCs.

Provision of Internet Facilities

4. Each centre must ensure that internet access enabled computer terminals are available to detainees 7 days a week for a minimum of 7 hours a day, though individual time slots may be limited if there is excessive demand.

5. Regulated access to the internet and any personal internet based email accounts will be provided to detainees, subject to the detainee 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 detainee has an insufficient knowledge of English to understand the acceptable use policy, the policy should be read to the detainee and explained in a language that they understand.

6. A decision to suspend internet access from a detainee can be taken by the supplier Centre/Deputy Centre Manager, for example for security or safety reasons or because a detainee is in breach of the centre's acceptable use policy on the use of the internet. A decision to suspend internet access must be recorded and the detainee notified in writing of the suspension and the reason for it. A decision to suspend should not be used as a sanction for wider non-compliance by a detainee.

7. The Home Office Immigration Enforcement (HOIE) 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 HOIE Manager and reviewed on a weekly basis until suspension has ended. The detainee can appeal any suspension, providing reasons in writing to the Centre/Deputy Centre Manager, who will make a

decision within 48 hours. For detainees with imminent removal directions, the decision should be made within 12 hours.

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

9. Centre suppliers should ensure that detainees are able to easily access any material on the internet that may be relevant to their immigration case as long as it does not fall within a prohibited category. This will include Home Office rules and guidance; court and tribunal proceedings and judgements; 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.

10. If a detainee has agreed to fund their own ticket to travel home, access to 'payment blocked' travel booking sites should be enabled for the detainee via the IRC welfare office. The detainee will be permitted to access any debit or credit card in their name that is in stored/valuable property. Once the transaction to purchase a ticket home has been completed the debit or credit card will be returned to the detainee's stored/valuable property.

11. The centre supplier must ensure that detainees 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 networking (including Facebook, Twitter, chat rooms and instant messaging)
    - Pornographic material
    - Dating
    - Gambling

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

12. The supplier should ensure that any detainee attempts to view, send or receive information related to prohibited harm related categories, sites or keywords/phrases is recorded and shared with the HOIE manager on a weekly basis. Where there is a serious incident such as attempts to access any extremist or radicalisation websites, the HOIE manager should be informed as soon as possible. A security information report must be completed in addition to a counter-terrorism referral where appropriate, as set out in DSO 11/2014, and emailed to the Detention Debrief Intelligence Team detentionservicesintelligenceteam@homeoffice.gsi.gov.uk. A summary of any

internet or email breaches should be submitted to the HOIE manager on a monthly basis.

13. Where a detainee requires access to a site that is likely to be prohibited regarding their immigration case, they should approach the welfare office to discuss access.

Adding and Removing Access to Individual Websites

14. A detainee can request access to a blocked website by making an application in writing to the centre supplier manager responsible for internet provision. The supplier will check the content of the website and, if it falls outside a prohibited category, the supplier will arrange for the detainee 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. The date and time of the request and when access was subsequently granted should be recorded by the supplier. If a detainee's request for access to a specific website is denied the detainee should be informed in writing of the decision by the centre supplier and the HOIE IRC team should be notified.

15. The supplier should complete a monthly log of all website access requests, both granted and denied, and submit to the Detention Services Freedom of Information inbox (DSFOI@homeoffice.gsi.gov.uk) for collation. The combined log from all centres will then be sent to each centre's internet administrator. On receipt of the log each supplier should review their centre's internet provision and take action to ensure that detainees 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 supplier has a concern with either adding or removing a specific website they should escalate to the HOIE Delivery Manager in the first instance.

Monitoring and Audit

16. The supplier 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 detainee. The centre's local Security Document should include a reference to IT and internet security.

17. Centre suppliers must ensure that all monitoring of electronic communications is compliant with Detention Centre Rule 27. Any electronic communications to or from a detainee containing privileged material (such as legal correspondence) must be excluded from all monitoring.

18. The internet room must be monitored by a member of supplier staff, 'the supervisor', at all times the room is in use. The supervisor must have appropriate IT skills and have received internet security awareness training prior to undertaking the role. The supervisor is responsible for monitoring all active internet sessions in the room in person 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. In order to ensure a manageable ratio between supervisor and terminals a supervisor should not monitor more than 30 terminals at any given time.

19. Following initial log on, detainees should not be able to swap terminals during their session and the supplier must ensure that there is a clear audit trail in place to match detainees 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 the supervisor must thoroughly inspect all terminals at the end of each session to ensure that all terminals are secure, recording the check in the wing or area diary.

20. Downloading or uploading of any files by a detainee is prohibited for security reasons. If a detainee wishes to print a document or email attachment the supplier 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 detainees 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 supplier's security manager.

Revision History

Review date	Reviewed by	Review outcome	Next review

Annex A

USE OF THE INTERNET – ACCEPTABLE USE POLICY

Use of the Internet

1. You are able to use the internet in this Centre, to help you to keep in contact with your friends and family and to prepare for your removal from the United Kingdom.

2. Staff are able to 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. A staff member assigned as the internet supervisor will monitor the use of the internet at all times the room is in use.

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

   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 number of 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.

- Protect your log-in and password at all times.

- 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.

- Co-operate with the internet supervisor at all times and obey any instructions given.

- Report any breach of this policy by yourself or others to the internet supervisor without delay.

You must not:

- Share your log-in or password details with any other detainee.

- Swap terminals with another user without logging off completely first and then re-connecting using your own log-in and password.

- Allow another detainee 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 or whether it 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