

OFFICIAL

DIRECTION TO CERTAIN AERODROME MANAGERS UNDER THE AVIATION SECURITY ACT 1982 RELATING TO SECURITY SCANNERS 2016

The Secretary of State, in exercise of the powers in sections 12(1)(a), 13(1), (2) and (3), 14(1A), and (3) and 15(1) and (4) of the Aviation Security Act 1982¹, and in accordance with Article 6 of Regulation (EC) No 300/2008 (more stringent measures applied by Member States) of the European Parliament and of the Council of 11th March 2008 on common rules in the field of civil aviation security² directs any person who is the manager of an aerodrome set out in Annex E to this direction as follows—

Citation, Commencement and Revocation

1. This Direction may be cited as the Security Scanners Direction 2016.
2. This Direction comes into force on 20 December 2016.
3. The following Directions are revoked—
 - a) the Security Scanners Direction 2015;
 - b) the Security Scanners (George Best Belfast City) Direction 2015;
 - c) the Security Scanners (Glasgow Prestwick Airport) Direction 2015; and
 - d) the Security Scanners (Liverpool John Lennon Airport) Direction 2015.

Interpretation

4. For the purposes of this Direction:

“Airport Operator” means the aerodrome manager of one of the aerodromes set out in Annex E to this Direction;

“security scanner” means the equipment used for the screening of persons, being equipment listed in accordance with paragraph 1 of Annex C of this Direction or otherwise permitted in accordance with paragraph 2 of Annex C.

Use of Security Scanners

5. The Airport Operator must deploy security scanner equipment such that every passenger is liable to selection for screening by security scanner in accordance with the provisions of this Direction.

¹ c. 36, amended by the Aviation and Maritime Security Act 1990 (c.31).

² OJ L 97, 9.4.2008, p.72.

OFFICIAL

More stringent measures applicable to existing requirements.

6. The legal requirements relating to the screening of persons applicable to the deployment of security scanners include the more stringent measures set out in Annex A to this Direction.

Code of Practice

7. The Airport Operator must ensure that, where security scanners are deployed, they are operated in accordance with the Code of Practice for Acceptable Use of Security Scanners in an Aviation Security Environment at Annex B to this Direction.

Public Operational Protocol

8. The Airport Operator must ensure that, where security scanners are deployed, they are operated in accordance with the Public Operational Protocol for the use of Security Scanners at Annex C to this Direction.

OFFICIAL-SENSITIVE Operational Protocol

9. The Airport Operator must ensure that, where security scanners are deployed, they are operated in accordance with the OFFICIAL-SENSITIVE Operational Protocol for the use of security scanners at Annex D to this Direction.

Signed:

**Head of Aviation Security Policy
Aviation Directorate
Department for Transport**

Dated: 31 October 2016

On behalf of the Secretary of State

OFFICIAL

Please note the separate handling instructions for the second part of this Annex.

ANNEX A

1) Regulation (EU) 2015/1998

The following additional measures shall apply:

In respect of points 1.3.1.1 and 4.1.1.2.:

Where security scanners are deployed for the screening of persons, the Airport Operator must comply with the provisions of the Security Scanners Direction 2016.

In respect of points 1.3.1.1 and 4.1.1.10.:

Persons who are selected to be screened by a security scanner and who opt out from being scanned must be screened in accordance with the provisions of the Security Scanners Direction 2016, Annex C, paragraph 10.

OFFICIAL-SENSITIVE

ANNEX A

OFFICIAL-SENSITIVE Part

**Code of Practice
for the Acceptable Use of Security Scanners in an
Aviation Security Environment**

October 2016

This Code of Practice sets out requirements for the use of security scanners at UK airports. Where security scanners are deployed, airport operators must ensure that the following measures are adopted.

Legal Authority

Airport Operators are required to operate security scanners pursuant to directions made by the Secretary of State for Transport under the Aviation Security Act 1982. These directions are available on the [gov.uk](https://www.gov.uk) website.

Privacy

An effective privacy policy must be put in place by the airport operator to protect individuals when being screened by security scanners. This must include the installation and use of Automatic Threat Recognition (ATR) software. ATR software interprets the scan data, instead of creating an image, and identifies areas where items may be concealed on the body. These areas are flagged on a standardised stick-figure on a screen, to indicate to the security officer areas of the individual's body which should receive a targeted hand-search (see separate guidance). Security staff must not be able to view images produced by the scanner which have not been interpreted by ATR.

Data Protection

Analysis shall be conducted by approved ATR algorithms. Immediately after the scanning analysis is completed and the individual moves away from the security scanner, all data relating to the individual must be destroyed, irretrievable and incapable of being copied or sent.

A communication to passengers must be available at the security screening area to inform them that "For the benefit of all passengers' security, passengers may be required to be screened using security scanner equipment. Assessment of the scan data will be conducted by a computer algorithm. No images of individuals are created, and no scan data will be saved."

Health and Safety

All security scanners must use millimetre wave technology, as it poses no known health and safety risks. Millimetre wave scanners utilise a very low power, non-ionising form of electromagnetic technology. Non-ionising radiation refers to electromagnetic waves which do not alter atoms in molecules by removing electrons. The amount of electromagnetic radiation emitted by millimetre wave security scanners is many times lower than that emitted by a mobile phone.

Alternatives

An individual may opt out of being scanned. In this instance, the individual must either be screened by an alternative method which includes at least an enhanced hand search in private or that individual must not be permitted to enter the security restricted area, or, if applicable, he or she must be removed from it. An enhanced hand search in private must take place in a private room or an area away from the main search comb. This may involve the loosening and/or removal of clothing.

Equipment Approval

Airport operators must discuss all prospective use of security scanners with the Department for Transport (DfT) before deployment to ensure that security standards are maintained.

Training

Security officers must obtain appropriate security clearances before receiving training in accordance with an appropriate package that takes account of all relevant guidance. Training packages should be developed in partnership with manufacturers and shared on request with the DfT or anyone authorised to act on behalf of the Secretary of State. Before being deployed to operate a security scanner, the security officer must have completed the appropriate training including how to deal with issues sensitively and to protect privacy. Records of training undertaken must be maintained and made available upon request by the DfT or anyone authorised to act on behalf of the Secretary of State.

Communications

An effective communication strategy must be developed to inform people of the security requirements where security scanners are deployed. It must be made clear at the earliest possible stage that all individuals selected for screening by a security scanner will be expected to be scanned. Individuals who refuse to be scanned must be offered an alternative screening method, involving at least an enhanced hand search in private. Information should be adequate, clear and provided ideally before any ticket purchase. In any event it must be provided prior to entering the passenger screening area. Information should also be readily available in a number of languages appropriate for the profile of passengers using the airport.

Selection Criteria

Individuals must not be selected on the basis of personal characteristics (i.e. on a basis that may constitute discrimination such as disability, sex, gender reassignment, age, race, religion or belief, pregnancy and maternity and sexual orientation). Airport Operators must also follow all the requirements relating to selection that are contained in the public and Official-Sensitive parts of the Security Scanner Direction.

Protocols

Security scanners must be operated in accordance with detailed protocols which contain the further information on the operation of the security scanner including selection criteria for those to be scanned. The security sensitive information is not published but must comply with the requirements contained in this Code of Practice.

Review

DfT shall continue to review this Code of Practice in light of operational experience and relevant changes in law.

This page is deliberately blank

PUBLIC OPERATIONAL PROTOCOL FOR THE USE OF SECURITY SCANNERS

Equipment

1. The security scanners which the Department for Transport (DfT) has approved for use by the Airport Operator are listed on the following GOV.UK webpage: <https://www.gov.uk/government/collections/aviation-security-screening-approved-equipment-list> (which may be updated from time to time).
2. Other security scanner equipment may be acceptable for use but only where the Airport Operator has received prior written permission to use the equipment from the Department for Transport (DfT).

Equipment Safety Checks

3. Prior to each operational use, the nominated person must ensure that the security scanning equipment is in correct working order. This includes ensuring that:
 - (a) all warning and operating lights are functional;
 - (b) the equipment is not visibly damaged; and
 - (c) all signage and staff support materials are in place.

Maintenance

4. Appropriately trained personnel must ensure that the security scanning equipment is subject to calibration verification in accordance with the manufacturer's instructions.

Equipment Failure

5. In the event of equipment failure, local rules apply and steps must be taken to rectify the problem as soon as practicable. A record must be maintained detailing the time and nature of the failure and the actions taken to effect rectification.
6. Records of equipment failure and any remedial action taken must be retained for a period of 12 months and made available on request to the DfT or persons authorised to act on behalf of the Secretary of State.

Screening Process

7. The security officer must explain to the individuals to be screened how they are required to present themselves for screening.
8. Individuals must be security scanned in a manner consistent with the manufacturer's instructions, and in accordance with applicable directions issued by the DfT, and taking account of applicable guidance and staff training.
9. After being screened by security scanner, un-cleared individuals must not be permitted to proceed into the security restricted area until such time as the security officer has identified and cleared any concerns.
10. An individual who has been selected to be screened by security scanner may opt out of being scanned but only if the individual being screened agrees to be searched by an alternative screening method, including at least an enhanced hand search in private. That search must take into account relevant guidance and may require the loosening and/or removal of clothing.
11. In the event that an individual declines to be scanned and refuses to undergo the alternative screening method of at least an enhanced hand search in private, the incident must be escalated to the appropriate member of security staff who will escort that individual landside and advise the passenger's airline that they have been refused access to the security restricted area and that the passenger should be offloaded. If appropriate, local processes for dealing with persons giving rise to security concerns should be followed.

OFFICIAL-SENSITIVE Annex

12. Security scanners must also be operated in accordance with the OFFICIAL-SENSITIVE protocol (Annex D of this Direction) which contains security sensitive information.

OFFICIAL-SENSITIVE

ANNEX D

OFFICIAL-SENSITIVE OPERATIONAL PROTOCOL FOR THE USE OF SECURITY SCANNERS

OFFICIAL

ANNEX E

This direction is made to the managers of the following aerodromes:

Aberdeen International
Belfast City (George Best)
Belfast International (Aldergrove)
Birmingham
Bristol
Cardiff
East Midlands
Edinburgh
Glasgow
Glasgow Prestwick
Leeds Bradford International
Liverpool (John Lennon)
London City Airport
London Gatwick
London Heathrow
London Luton
London Southend
London Stansted
Manchester
Newcastle International
Southampton