DIRECTION TO THE AIRPORT OPERATOR OF LONDON CITY AIRPORT UNDER THE AVIATION SECURITY ACT 1982 RELATING TO SECURITY SCANNERS 2012

The Secretary of State, in exercise of the powers conferred under sections 12(1) and (6),13(1) and (2)(c),14(1A), 2(b) and (3), 15(1) and (4), 17(1) and 38(6) of the Aviation Security Act 1982[1] for the purposes to which Part II of the Act applies, 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 security[2] directs the airport operator of London City Airport as follows:

Citation and Commencement

1. This Direction may be cited as the Security Scanners (London City Airport) Direction 2012.

2. This Direction comes into force on 12 July 2012.

Interpretation

3. For the purposes of this Direction:

   "the Airport Operator" means the Airport Operator of London City Airport;

   "security scanner" means the equipment used for the screening of passengers which complies with the requirements in paragraph 1 of Annex C of this Direction.

Use of Security Scanners

4. The Airport Operator must ensure that security scanner equipment is deployed in accordance with this Direction at London City Airport no later than 1st September 2012.

5. The Airport Operator may deploy security scanner equipment at London City Airport before 1st September 2012 in accordance with this Direction.

More stringent measures applicable to existing requirements

6. The existing requirements relating to the screening of passengers are amended to the extent as set out in Annex A to 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.

Code of Practice

7. The Airport Operator shall ensure that, where security scanners are deployed, the Code of Practice for Acceptable Use of Security Scanners in an Aviation Security Environment, attached as Annex B to this Direction, shall be followed.

Public Protocol

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

Restricted Protocol

9. The Airport Operator shall ensure that where security scanners are deployed they are operated in accordance with the Restricted Operational Protocol for the use of security scanners at London City Airport attached as Annex D to this Direction.

Signed:

Tim Figures
Head of Division
Aviation Security Division
Department for Transport

Dated: 12 July 2012

On behalf of the Secretary of State

ANNEX A

For the purposes of this Direction, the following more stringent measures shall be applicable to London City Airport in respect of the following existing requirements:

Commission Regulation (EU) No 185/2010, Annex

Chapter 4

Screening of passengers

Point 4.1.1.10

Passengers who are selected for scanning in accordance with the Security Scanners (London City Airport) Direction 2012 to be screened by a security scanner and who opt out from being scanned may not be screened by an alternative screening method and will therefore not be permitted to proceed to the security restricted area (the Critical Part), with the result that they will not be permitted to fly on that occasion.

Single Consolidated Direction (Aviation) 2010

Chapter 4 Part A

4.1.1 Screening of Passengers

Point 4.1.1.2

All rescreening of passengers shall be conducted by means of a hand search or a security scanner in accordance with the Security Scanners (London City Airport) Direction 2012.

ANNEX A
Restricted Part

ANNEX B

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

November 2011

The Department for Transport has actively considered the needs of blind and partially sighted people in accessing this document. The text will be made available in full on the Department's website in accordance with the W3C's Web Content Accessibility Guidelines. The text may be freely downloaded and translated by individuals or organisations for conversion into other accessible formats. If you have other needs in this regard please contact the Department.

Department for Transport
Great Minster House
33 Horseferry Road
London SW1P 4DR
Telephone 020 7944 8300
Website www.dft.gov.uk

To order further copies contact:
DfT Publications
Tel: 0300 123 1102
www.dft.gov.uk/orderingpublications

Printed in Great Britain on paper containing at least 75% recycled fibre

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

Airports will operate security scanners as set out in Directions made on behalf of the Secretary of State for Transport under the Aviation Security Act 1982. These Directions are available on the Department for Transport web site.

Privacy

An effective privacy policy must be put in place by the airport operator to protect passengers when being screened by security scanners. As approved automatic threat recognition (ATR) software becomes available, it should be fitted to all new purchases of equipment. Where ATR software is not being used the privacy policy must include a requirement that the equipment is sited in such a way to ensure that the security screener(s) conducting analysis of the image (the screener) must not be able to see the person whose image they are viewing and the security screener(s) resolving any issues identified by the security scanner should not be able to see the image of the person being searched. The policy must also include procedures to ensure that image-capturing equipment (such as cameras and mobile phones) is not taken into the viewing room and that images are not left on unattended screens.

A person selected for scanning may request that the screen reader is of the same sex and the airport must meet this request as quickly as possible. If further resolution is required (i.e. a targeted hand search), an appropriate method of communication must be employed between the screen reader and the security searcher that does not include the use of the image to ensure that this privacy is protected.

Data Protection

In order to classify a passenger's security status when using a security scanner, it is necessary to capture data for analysis. Airport operators shall ensure that checks are undertaken at least twice yearly to ensure that data cannot be saved, copied or sent. Any facilities on the scanner which could be used to retain, copy or transmit data must be disabled. The scanning process shall comply with the general law on data protection.

Analysis can be conducted by a security screener and/or by approved automatic threat recognition software.

Immediately after the scanning analysis is completed and the passenger moves away from the security scanner, all data relating to the passenger must be destroyed and irretrievable. Whilst an image is being analysed, it must only be possible for the screener to view that image. In exceptional circumstances where a screener believes there is a viable threat to the safety of passengers or staff, an additional appropriate security screener may be required to view the image. There must be no method of copying or transferring images.

Communications will be available at the security screening area to inform passengers that "For the benefit of all passengers' security, passengers may be required to be screened using security scanning equipment. Screening will be conducted by security screeners acting on behalf of the airport operator. Images of passengers will not be saved." Airport operators must provide to persons selected for screening the opportunity to provide details of their age, gender, race, ethnic origin and religion or beliefs.

Health and Safety

The Department for Transport ("DfT") has the results of an independent assessment of the risks to health from the effects of security scanners that utilise ionising radiation technology. This assessment provides evidence that the use of such security scanners represents a negligible risk to health from exposure to ionising radiation. The assessment compares the risk from security scanners to other everyday risks and is available via the DfT website (http://www.dft.gov.uk/pgr/security/aviation/airport/). Assessments completed by authorities outside of the UK have concluded that the risks to health from security scanners using very low dose ionising radiation is so low as to be negligible.

The airport authority deploying a security scanner must ensure that all appropriate local risk assessments have been conducted for the type of security scanner being deployed and that the equipment conforms to all relevant health and safety requirements. Before deployment of security scanners that produce ionising radiation, a measure of the ambient radiation dosage and the effective dose that a passenger receives when being scanned, must be conducted by qualified persons. Local rules must be agreed and applied to mitigate the risks that a security scanner is used outside of normal operating conditions (whether through incorrect use or malfunction).

Equipment Approval

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

Training

Security screeners must obtain appropriate security clearances before receiving training and receive training in accordance with an approved package. Training packages should be developed in partnership with manufacturers and must be approved by the DfT. Before being deployed to operate a security scanner, a security screener 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.

Communications

An effective communication strategy should be developed to inform people of the security requirements where security scanners are deployed. It should be made clear at the earliest possible stage that all passengers selected for screening by a security scanner must be scanned. If a passenger declines to be scanned that passenger must be refused access to the restricted area of the airport (the Critical Part), with the result that the passenger will not be able to fly on that occasion. Information should be adequate, clear and provided ideally before 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

Passengers 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). Airports must also follow all the requirements relating to selection that are contained in the public and restricted parts of the security scanner Direction.

The passenger shall be informed that they have been selected for scanning in order to resolve security concerns or have been selected at random, except where selection is done by automated means.

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 will comply with the requirements contained in this Code of Practice.

Review

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

ANNEX C

PUBLIC OPERATIONAL PROTOCOL FOR THE USE OF SECURITY SCANNERS AT LONDON CITY AIRPORT

EQUIPMENT

1. The following equipment shall be suitable for use:

   (a) L3 Communications ProVision,
   (b) Smiths Detection "eqo", and
   (c) any other equipment accepted for use in writing by the Department for Transport (DfT) before deployment.

Equipment Safety Checks

2. Prior to operational use, the nominated person shall ensure that the security scanning equipment is in correct working order. This shall include ensuring that:

   - all warning and operating lights are functional;
   - that the equipment is not visibly damaged, and
   - that all signage and staff support materials are in place.

Maintenance

3. Appropriately trained personnel shall maintain the security scanning equipment in accordance with the manufacturer's instructions. Records of maintenance shall be maintained and made available to the DfT upon request.

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

Equipment Failure

5. In the event of equipment failure, local rules shall apply and steps shall be taken to rectify the problem as soon as practicable. A record shall be maintained detailing the time and nature of the failure and the actions taken to effect rectification.

Selection Criteria

6. Passengers may only be selected for scanning in accordance with searching and screening requirements set out in this Direction.

7. Passengers shall be scanned if one of the following criteria apply:

(a) they have requested an alternative search method prior to or after passing through the walk-through metal detection (WTMD) equipment.

(b) they have been referred for alarm resolution by scanning following a WTMD alarm or in the instance that the security screener believes that further investigation is required following completion of the hand search process;

(c) they have been referred for security scanning following an evidence-based assessment of behaviour that gives cause to the assessor to believe that a scan is warranted;

(d) they have been selected by explosive detection dogs;

(e) they have caused explosive detection equipment to activate; or

(f) they are selected at random on a continuous basis without regard to personal characteristics (i.e. not on a basis that may constitute unlawful discrimination such as: disability, gender, gender reassignment, race, age, religion or belief or sexual orientation).

Passenger Scanning Process

8. All security scanners that are deployed shall be operated for the duration of the operational day.

9. All security scanners that are deployed shall be operated on a continuous basis.

10. Any passenger who is selected for scanning shall be escorted to the security scanner by a security screener or supervisor.

11. Screen operators may view images of both genders but a passenger selected for scanning may request that the screen reader is a person of the same sex.

12. The scanning process shall take place in a way which safeguards a passenger's privacy by ensuring that the screen reader does not see the passenger.

13. The security screener shall explain to the passenger that they have been selected for additional screening in order to resolve security concerns or that they have been selected at random unless selected by automated means. The security screener shall explain the process to the passenger using translation cards if needed.

14. If a passenger who has been selected for scanning declines to be scanned in accordance with the Security Scanners (London City) Direction 2012, that passenger shall not be permitted to proceed to the security restricted area (the Critical Part), with the result that he or she will not be permitted to fly on that occasion.

15. The security screener shall provide safety information as required by legislation or if otherwise requested.

16. If required, walking sticks may be taken into the security scanner and passengers shall be scanned to the best possible standard. Children may hold the hand of their parent or guardian whilst being scanned if possible.

17. Passengers shall be security scanned in a manner consistent with the manufacturer's instructions and staff training.

18. After being scanned, cleared passengers shall be allowed to leave the security scanning area.

19. After being scanned, un-cleared passengers shall not be permitted to proceed into the security restricted area until such time as the security screener has identified and cleared any concerns.

20. In the event that a passenger declines to be scanned, the incident shall be escalated to the appropriate member of Security Staff who shall escort the passenger 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. In the instance of suspicious circumstances police support shall be requested. The appropriate member of Security Staff may if necessary ensure that the police are aware of the circumstances.

Restricted Annex

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

ANNEX D

RESTRICTED OPERATIONAL PROTOCOL FOR THE USE OF SECURITY SCANNERS AT GATWICK AIRPORT

DIRECTION TO THE AIRPORT OPERATOR OF STANSTED AIRPORT UNDER THE AVIATION SECURITY ACT 1982 RELATING TO SECURITY SCANNERS 2012

The Secretary of State, in exercise of the powers conferred under sections 12(1) and (6),13(1) and (2)(c),14(1A), 2(b) and (3), 15(1) and (4), 17(1) and 38(6) of the Aviation Security Act 1982[1] for the purposes to which Part II of the Act applies, 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 security[2] directs the airport operator of Stansted Airport as follows:

Citation and Commencement

1. This Direction may be cited as the Security Scanners (Stansted Airport) Direction 2012.

2. This Direction comes into force on 25 October 2012.

Interpretation

3. For the purposes of this Direction:

   "the Airport Operator" means the Airport Operator of Stansted Airport;

   "security scanner" means the equipment used for the screening of passengers which complies with the requirements in paragraph 1 of Annex C of this Direction.

Use of Security Scanners

4. The Airport Operator must deploy security scanner equipment at Stansted Airport in accordance with this Direction no later than 25 October 2012.

More stringent measures applicable to existing requirements

5. The existing requirements relating to the screening of passengers are amended to the extent as set out in Annex A to 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.

Code of Practice

7. The Airport Operator shall ensure that, where security scanners are deployed, the Code of Practice for Acceptable Use of Security Scanners in an Aviation Security Environment, attached as Annex B to this Direction, shall be followed.

Public Protocol

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

Restricted Protocol

9. The Airport Operator shall ensure that where security scanners are deployed they are operated in accordance with the Restricted Operational Protocol for the use of security scanners at Stansted Airport attached as Annex D to this Direction.

Signed:

David Elbourne
Head of Regulation
Aviation Security Division
Department for Transport

Dated: 24 October 2012

On behalf of the Secretary of State

ANNEX A

For the purposes of this Direction, the following more stringent measures shall be applicable to Stansted Airport in respect of the following existing requirements:

Commission Regulation (EU) No 185/2010, Annex

Chapter 4

Screening of passengers

Point 4.1.1.10

Passengers who are selected for scanning in accordance with the Security Scanners (Stansted Airport) Direction 2012 to be screened by a security scanner and who opt out from being scanned may not be screened by an alternative screening method and will therefore not be permitted to proceed to the security restricted area (the Critical Part), with the result that they will not be permitted to fly on that occasion.

Single Consolidated Direction (Aviation) 2010

Chapter 4 Part A

4.1.1 Screening of Passengers

Point 4.1.1.2

All rescreening of passengers shall be conducted by means of a hand search or a security scanner in accordance with the Security Scanners (Stansted Airport) Direction 2012.

ANNEX A
Restricted Part

ANNEX B

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

November 2011

The Department for Transport has actively considered the needs of blind and partially sighted people in accessing this document. The text will be made available in full on the Department's website in accordance with the W3C's Web Content Accessibility Guidelines. The text may be freely downloaded and translated by individuals or organisations for conversion into other accessible formats. If you have other needs in this regard please contact the Department.

Department for Transport
Great Minster House
33 Horseferry Road
London SW1P 4DR
Telephone 020 7944 8300
Website www.dft.gov.uk

To order further copies contact:
DfT Publications
Tel: 0300 123 1102
www.dft.gov.uk/orderingpublications

Printed in Great Britain on paper containing at least 75% recycled fibre

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

Airports will operate security scanners as set out in Directions made on behalf of the Secretary of State for Transport under the Aviation Security Act 1982. These Directions are available on the Department for Transport web site.

Privacy

An effective privacy policy must be put in place by the airport operator to protect passengers when being screened by security scanners. As approved automatic threat recognition (ATR) software becomes available, it should be fitted to all new purchases of equipment. Where ATR software is not being used the privacy policy must include a requirement that the equipment is sited in such a way to ensure that the security screener(s) conducting analysis of the image (the screener) must not be able to see the person whose image they are viewing and the security screener(s) resolving any issues identified by the security scanner should not be able to see the image of the person being searched. The policy must also include procedures to ensure that image-capturing equipment (such as cameras and mobile phones) is not taken into the viewing room and that images are not left on unattended screens.

A person selected for scanning may request that the screen reader is of the same sex and the airport must meet this request as quickly as possible. If further resolution is required (i.e. a targeted hand search), an appropriate method of communication must be employed between the screen reader and the security searcher that does not include the use of the image to ensure that this privacy is protected.

Data Protection

In order to classify a passenger's security status when using a security scanner, it is necessary to capture data for analysis. Airport operators shall ensure that checks are undertaken at least twice yearly to ensure that data cannot be saved, copied or sent. Any facilities on the scanner which could be used to retain, copy or transmit data must be disabled. The scanning process shall comply with the general law on data protection.

Analysis can be conducted by a security screener and/or by approved automatic threat recognition software.

Immediately after the scanning analysis is completed and the passenger moves away from the security scanner, all data relating to the passenger must be destroyed and irretrievable. Whilst an image is being analysed, it must only be possible for the screener to view that image. In exceptional circumstances where a screener believes there is a viable threat to the safety of passengers or staff, an additional appropriate security screener may be required to view the image. There must be no method of copying or transferring images.

Communications will be available at the security screening area to inform passengers that "For the benefit of all passengers' security, passengers may be required to be screened using security scanning equipment. Screening will be conducted by security screeners acting on behalf of the airport operator. Images of passengers will not be saved." Airport operators must provide to persons selected for screening the opportunity to provide details of their age, gender, race, ethnic origin and religion or beliefs.

Health and Safety

The Department for Transport ("DfT") has the results of an independent assessment of the risks to health from the effects of security scanners that utilise ionising radiation technology. This assessment provides evidence that the use of such security scanners represents a negligible risk to health from exposure to ionising radiation. The assessment compares the risk from security scanners to other everyday risks and is available via the DfT website (http://www.dft.gov.uk/pgr/security/aviation/airport/). Assessments completed by authorities outside of the UK have concluded that the risks to health from security scanners using very low dose ionising radiation is so low as to be negligible.

The airport authority deploying a security scanner must ensure that all appropriate local risk assessments have been conducted for the type of security scanner being deployed and that the equipment conforms to all relevant health and safety requirements. Before deployment of security scanners that produce ionising radiation, a measure of the ambient radiation dosage and the effective dose that a passenger receives when being scanned, must be conducted by qualified persons. Local rules must be agreed and applied to mitigate the risks that a security scanner is used outside of normal operating conditions (whether through incorrect use or malfunction).

Equipment Approval

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

Training

Security screeners must obtain appropriate security clearances before receiving training and receive training in accordance with an approved package. Training packages should be developed in partnership with manufacturers and must be approved by the DfT. Before being deployed to operate a security scanner, a security screener 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.

Communications

An effective communication strategy should be developed to inform people of the security requirements where security scanners are deployed. It should be made clear at the earliest possible stage that all passengers selected for screening by a security scanner must be scanned. If a passenger declines to be scanned that passenger must be refused access to the restricted area of the airport (the Critical Part), with the result that the passenger will not be able to fly on that occasion. Information should be adequate, clear and provided ideally before 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

Passengers 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). Airports must also follow all the requirements relating to selection that are contained in the public and restricted parts of the security scanner Direction.

The passenger shall be informed that they have been selected for scanning in order to resolve security concerns or have been selected at random, except where selection is done by automated means.

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 will comply with the requirements contained in this Code of Practice.

Review

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

ANNEX C

PUBLIC OPERATIONAL PROTOCOL FOR THE USE OF SECURITY SCANNERS AT STANSTED AIRPORT

EQUIPMENT

1. The following equipment shall be suitable for use:

   (a) L3 Communications ProVision,
   (b) Smiths Detection "eqo", and
   (c) any other equipment accepted for use in writing by the Department for Transport (DfT) before deployment.

Equipment Safety Checks

2. Prior to operational use, the nominated person shall ensure that the security scanning equipment is in correct working order. This shall include ensuring that:

   - all warning and operating lights are functional;
   - that the equipment is not visibly damaged, and
   - that all signage and staff support materials are in place.

Maintenance

3. Appropriately trained personnel shall maintain the security scanning equipment in accordance with the manufacturer's instructions. Records of maintenance shall be maintained and made available to the DfT upon request.

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

Equipment Failure

5. In the event of equipment failure, local rules shall apply and steps shall be taken to rectify the problem as soon as practicable. A record shall be maintained detailing the time and nature of the failure and the actions taken to effect rectification.

Selection Criteria

6. Passengers may only be selected for scanning in accordance with searching and screening requirements set out in this Direction.

7. Passengers shall be scanned if one of the following criteria apply:

(a) they have requested an alternative search method prior to or after passing through the walk-through metal detection (WTMD) equipment.

(b) they have been referred for alarm resolution by scanning following a WTMD alarm or in the instance that the security screener believes that further investigation is required following completion of the hand search process;

(c) they have been referred for security scanning following an evidence-based assessment of behaviour that gives cause to the assessor to believe that a scan is warranted;

(d) they have been selected by explosive detection dogs;

(e) they have caused explosive detection equipment to activate; or

(f) they are selected at random without regard to personal characteristics (i.e. not on a basis that may constitute unlawful discrimination such as: disability, gender, gender reassignment, race, age, religion or belief or sexual orientation).

Passenger Scanning Process

8. All security scanners shall be operational for the duration of the day and the airport operator shall screen passengers on a random basis in accordance with this Protocol.

9. Any passenger who is selected for scanning shall be escorted to the security scanner by a security screener or supervisor.

10. Screen operators may view images of both genders but a passenger selected for scanning may request that the screen reader is a person of the same sex.

11. The scanning process shall take place in a way which safeguards a passenger's privacy by ensuring that the screen reader does not see the passenger.

12. The security screener shall explain to the passenger that they have been selected for additional screening in order to resolve security concerns or that they have been selected at random unless selected by automated means. The security screener shall explain the process to the passenger using translation cards if needed.

13. If a passenger who has been selected for scanning declines to be scanned in accordance with the Security Scanners (Stansted Airport) Direction 2012, that passenger shall not be permitted to proceed to the security restricted area (the Critical Part), with the result that he or she will not be permitted to fly on that occasion.

14. The security screener shall provide safety information as required by legislation or if otherwise requested.

15. If required, walking sticks may be taken into the security scanner and passengers shall be scanned to the best possible standard. Children may hold the hand of their parent or guardian whilst being scanned if possible.

16. Passengers shall be security scanned in a manner consistent with the manufacturer's instructions and staff training.

17. After being scanned, cleared passengers shall be allowed to leave the security scanning area.

18. After being scanned, un-cleared passengers shall not be permitted to proceed into the security restricted area until such time as the security screener has identified and cleared any concerns.

19. In the event that a passenger declines to be scanned, the incident shall be escalated to the appropriate member of Security Staff who shall escort the passenger 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. In the instance of suspicious circumstances police support shall be requested. The appropriate member of Security Staff may if necessary ensure that the police are aware of the circumstances.

Restricted Annex

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

ANNEX D

RESTRICTED OPERATIONAL PROTOCOL FOR THE USE OF SECURITY SCANNERS AT GATWICK AIRPORT