



Policy name: Managing Conveyance of Unauthorised and Illicit Items Policy Framework (Closed Prisons)

Re-issue Date: 21 November 2024

Implementation Date: 10th January 2025*

*Prisons can choose to implement the policy ahead of this date

Replaces the following documents which are hereby cancelled:

- PSI 10/2012 Conveyance and Possession of Prohibited Items and other Related Offences.
- PSI 21/2015 Unauthorised Possession within Prisons of Knives and other Offensive Weapons.
- NOMS Security Management Specification 1, 2, 3, 13, 14, 16, 17
- NOMS Prisoner Comms Specification 10.
- NOMS Comms Control Room Specification 6,7,8,11,18.
- NOMS Gate Services Specification 1, 2, 4, 5, 6, 7, 9, 11, 12, 13, 15 & 16.

Action required by:

X	HMPPS HQ	X	Governors
X	Public Sector Prisons	X	Heads of Group
X	Contracted Prisons		The Probation Service
X	Under 18 Young Offender Institutions		Other providers of Probation and Community Services
	HMPPS Rehabilitation Contract Services Team		

Mandatory Actions: All groups referenced above must adhere to the Requirements section of this Policy Framework, which contains all mandatory actions.

For Information: By the implementation date, Governors of public sector prisons and contracted prisons must ensure that their local procedures do not contain references to:

- PSI 14/2011 Management and Security of Gate Services.
- PSI 13/2011 Management and Security of Communication/Control Rooms and Internal Prisoner Movement.
- PSI 10/2012 Conveyance and Possession of Prohibited Items and other Related Offences.
- PSI 21/2015 Unauthorised Possession within Prisons of Knives and other Offensive weapons.

Governors must ensure that any new local policies developed as a result of this Policy Framework are compliant with relevant legislation, including the Public Sector Equality Duty (Equality Act 2010).

OFFICIAL

Section 6 of the Policy Framework contains Guidance to assist implementation of the Requirements set out in Section 4.

Terminology

In this document:

- The term Governor also applies to Directors of contracted prisons.
- The word 'unauthorised' relates to items which a person is not authorised by the Governor to have in possession and could lead to disciplinary action.
- The word 'illicit' relates to items for which it is a criminal offence to have in possession and could lead to prosecution.
- The word 'find' relates to the discovery of an illicit or unauthorised item during a search procedure.
- An offensive weapon within the [Police and Criminal Evidence Act 1984](#) is defined as "any article made or adapted for use for causing injury to persons; or intended by the person having it with him for such use by him or by some other person". As such, this also includes all makeshift weapons which are manufactured from items within prisons.

How will this Policy Framework be audited or monitored:

In public sector prisons, Prison Group Directors (PGDs) will monitor compliance with requirements set out within the Policy Framework in their prisons using the auditing and monitoring tools described in this framework. In contracted prisons, monitoring of compliance will be through the standard contract management processes.

Health and Safety for public sector prisons is undertaken through Health and Safety monitoring and assurance. The Health and Safety processes may be different for contracted prisons and therefore, contracted prisons must have their own Health and Safety arrangements which must ensure, so far as is reasonably practicable, the health, safety, and welfare at work of all employees.

Quality assurance for public sector prisons and contracted prisons is provided by HMPPS Performance, Assurance & Risk (PAR) Group through the security audit.

Resource Impact:

The identified resource impact for this Policy Framework is staffing within the Security Department. The initial impact will be time taken to update the Local Security Strategy (LSS) in alignment with this Policy Framework. Prisons will also have to conduct a whole prison approach evidence-based risk assessment to identify their risks of conveyance and update their LSS to reflect these. Following that, resource implication is not expected to be any different to current requirements.

There will be an additional resource impact for prisons with Enhanced Gate Security (EGS) ensuring key roles and responsibilities are fulfilled.

Contact: security.procedures@justice.gov.uk

Deputy/Group Director sign-off: Andy Rogers, Deputy Director, Operational Security Group, Directorate of Security.

Approved by OPS for publication: Helen Judge, Joint Chair, Operational Policy Sub-board, July 2024.

OFFICIAL

Revisions

Date	Changes
30 August 2024	Clarifications made to paragraphs 4.4.21 and 6.3.19.
21 November 2024	Amendments made to para 4.4.43 and 4.4.44

OFFICIAL

Contents

Section	Title	Page
1	Purpose	5
2	Evidence	5
3	Outcomes	5
4	Requirements 4.1 Management of Conveyance General 4.2 Prison Act 1952, Crown Immunity and Criminal Liability 4.3 Authorisations for Conveyance of Items (Central and Local) 4.4 Management of Conveyance via Gate (including Enhanced Gate Security) 4.5 Management of Conveyance via Prisoner Reception 4.6 Management of Conveyance via Correspondence 4.7 Management of Conveyance via the Perimeter 4.8 Management of Conveyance via Visits 4.9 Conveyance of Medication 4.10 Long Term High Security Estate & Restricted Status Prisoners 4.11 Police Referrals	6
5	Constraints	28
6	Guidance 6.1 Management of Conveyance General 6.2 Criminal Liability and Authorisations 6.3 Guidance on Managing Conveyance via Gate (including Enhanced Gate Security) 6.4 Guidance on Managing Conveyance via Reception 6.5 Guidance on Managing Conveyance via Correspondence 6.6 Guidance on Managing Conveyance via Perimeter 6.7 Guidance on Managing Conveyance via Visits 6.8 Guidance on Safety Considerations	29
7	Annexes	49

OFFICIAL

1. **Purpose**

- 1.1 This Policy Framework provides closed public sector and contracted prisons with the information and guidance needed to manage the conveyance of illicit items into and out of prisons, ultimately supporting a safe and secure environment for staff, visitors, and prisoners.
- 1.2 The Policy Framework links to:
- Rule 70 of the Prison Rules 1999 (Prohibited Articles) “No person shall, without authority, convey into or throw into or deposit in a prison, or convey or throw out of a prison, or convey to a prisoner, or deposit in any place with intent that it shall come into the possession of a prisoner, any article whatever. Anything so conveyed, thrown, or deposited may be confiscated by the governor.”
 - Rule 74 of the YOI Rules 2000 Prohibited Articles “No person shall, without authority, convey into or throw into or deposit in a young offender institution, or convey to an inmate, or deposit in any place with intent that it shall come into the possession of an inmate, any article whatsoever. Anything so conveyed, thrown, or deposited may be confiscated by the governor”.
 - Prison Rule 70A/YOI Rule 74A introduced to provide a List C of controlled items in accordance with section 40A (6) Prison Act 1952.

2. **Evidence**

- 2.1 His Majesty’s Prison and Probation Service (HMPPS) seeks to protect prisoners, those working in or visiting prisons, and the general public by taking steps to prevent the conveyance and supply of illicit items into prisons. Illicit items can drive and contribute to violence, debt, bullying, and ongoing criminality in prisons; all of which undermine safety, security, public confidence, and rehabilitation.
- 2.2 Evidence shows that some people seek to undermine security measures by conveying illicit items into prisons through varying routes, particularly the gate, reception, correspondence, perimeter, and visits. Data on finds of illicit items is published annually via the HMPPS Annual Digest at www.gov.uk.
- 2.3 HMPPS has undertaken several steps to disrupt the supply of illicit items into prisons. Importantly, security procedures and practices, when carried out effectively can assist in preventing routes of conveyance, helping to create a safer and more secure environment for rehabilitation.

3. **Outcomes**

- 3.1 By following the requirements and information in this Policy Framework, staff working in prisons will be able to:
- Detect and deter crimes and threats to the security, order, and control of the prison.
 - Identify conveyance risk and improve capability to detect illicit and unauthorised items attempting to enter prisons via the gate, reception, correspondence, perimeter, and visits.
 - Deter the exploitation of visitors, staff, and prisoners to convey illicit and unauthorised items into prisons.
 - Ensure only authorised persons, vehicles, goods enter and leave the prison.
 - Ensure tighter control of items being brought into, taken out of, and possessed within prison in line with the Prison Act 1952.

OFFICIAL

4. **Requirement**

4.1 **Management of Conveyance General (see Guidance 6.1 for supporting information)**

Local assessment

- 4.1.1 Governors must ensure that they conduct an annual evidence-based assessment to identify and manage the risks of conveyance locally as per the [Local Security Strategy Policy Framework](#). Any local arrangements decided upon must be consistent with the instructions provided in this Policy Framework and support a rehabilitative culture.
- 4.1.2 Organised Crime Group (OCG) prisoners can be key drivers of conveyance. Such prisoners and their connections should be factored in as part of any local assessment and mitigating actions. The [Serious and Organised Crime Policy Framework](#) and Serious Organised Crime Unit can support prisons in considering actions for the management of such nominals.
- 4.1.3 Whilst individual measures may not permanently stop a route of conveyance, they can interrupt or reduce it. Prisons however should be aware of the possibility of displacing risks in that by tackling one area, another route of conveyance or risk may arise.

Local Security Strategy

- 4.1.4 Following an evidence-based risk assessment, Governors must ensure the Local Security Strategy (LSS) is updated and outlines effective procedures for addressing each conveyance risk area.
- 4.1.5 Governors must ensure the LSS is communicated to all staff (including not directly employed), so they are aware of their role in managing security in respect of conveyance and have access to necessary information to prevent illicit items entering a prison and to help detect those that have already entered.
- 4.1.6 Governors must ensure that a nominated person is responsible for updating the LSS. This must include regular oversight of the risk of conveyance and the related assessment process to consider emerging and changing risks.

Assurance

- 4.1.7 Governors must put effective assurance processes in place to identify and address any weaknesses or vulnerabilities in procedures that have been identified to reduce the risks of conveyance. Governors must ensure covert testing as an additional assurance measure is carried out as per the [Covert Testing Policy Framework \(to be published\)](#).

Notifications and Communications

- 4.1.8 Governors must ensure that signs laying out penalties for committing offences under the Prison Act 1952 covered in this Framework are clearly displayed outside the prison, normally at the point of entrance to the prison. Briefings and information notices must also be made available to prisoners (for example in libraries), staff, and social and professional visitors (for example at the gate). See Template Notice – Criminal Acts of Conveyance (Annex C) and Template Notice – Consequences of Conveyance (Annex D).
- 4.1.9 Governors must ensure that the list of prohibited items is available to staff, prisoners, and visitors on entry to the prison. Only authorised items are permitted in and out of the prison.

OFFICIAL

Items which are not permitted are set out in List A, B and C items (Annex A), in addition to any local lists.

- 4.1.10 Governors must ensure that conveyance of unauthorised/illicit items is discussed with managers and staff of contract/service providers including healthcare and education (e.g., during induction, local training), to ensure that the implication for their staff is fully understood and action taken where required.

Reporting and Evidence Management

- 4.1.11 Illicit and unauthorised items found must be reported via an Intelligence Report (IR) as per [Intelligence Collection, Management and Dissemination in Prisons and Probation Policy Framework](#). Reporting of illicit and unauthorised items found as part of a search must also include the Incident Reporting System (IRS) as per the [Incident Management Policy Framework \(Restricted\)](#). Governors must also consider adjudication procedures for any items found on prisoners in line with the [Prison Adjudication Policy Framework](#).
- 4.1.12 Governors must ensure staff follow set procedures for the preservation of evidence as set out in [Management and Handling of Evidence Policy Framework](#) and [Prisoners' Property Policy Framework](#) when illicit items are found in a prisoner's possession or within the prison.
- 4.1.13 Any material found that could pose a terrorist risk must be reported via an I.R and seized for review by the prisons Counter Terrorism Unit or Regional Counter Terrorism Team. See [Managing Extremism and Terrorism Among Offenders in Custody and the Community Policy Framework \(Restricted\)](#) for further information.

4.2 Prison Act 1952, Crown Immunity and Criminal Liability (see Guidance 6.2 for supporting information)

- 4.2.1 The [Prison Act 1952](#) ("Prison Act") sets out the legislation under the section offences. The Act sets out the penalties for each of the offences listed below:
- **39.** Assisting a prisoner to escape.
 - **40A.** Classification of articles within 40B and 40C.
 - **40B.** Conveyance of List A articles into or out of prison.
 - **40C.** Conveyance of List B or C articles into or out of prison.
 - **40CA.** Unauthorised possession in prison of knife or offensive weapon.
 - **40CB.** Throwing articles into prison.
 - **40D.** Other offences relating to prison security.
 - **40E.** Section 40D: meaning of "authorisation" and other interpretation.
 - **40F.** Offences under sections 40B to 40D: extension of Crown immunity.
- 4.2.2 There are three main situations in which criminal liability for the offences listed above will not arise:
- When Crown immunity for Crown Servants is available.
 - Under an extension of Crown immunity which is provided for by the Act for non-Crown Servants.
 - Where there is an explicit written authorisation under sections 40B (for list A items) or 40E (for other items) of the Prison Act.

OFFICIAL

4.3 Authorisations for Conveyance of Items – Central and Local (see Guidance 6.2 for supporting information)

- 4.3.1 Section 40B and 40E of the Prison Act provides powers for the Secretary of State or by a senior official to authorise any person or group of people to convey into or out of the prison or use or possession in the prison any item which may be prohibited by Section 40B to 40D of the Prison Act from being so conveyed or used.
- 4.3.2 Section 40E of the Prison Act provides powers to Governors or Directors of contracted prisons to grant authorisation to any person or group of people to convey into or out of the prison or use in the prison any item which may be prohibited by Section 40B to 40D of the Prison Act from being so conveyed or used or possessed. Governors (or PGDs) must authorise List A items. PGDs must always authorise mobile phones (List B). Other items may be authorised by any person working at the prison who the Governor has authorised to grant S40E authorisations on their behalf.
- 4.3.3 Where the activity does not form part of a person's normal duties (and therefore Crown immunity would not be available), there must be specific authorisation under the terms of section 40B (for list A items) or 40E (for other authorisations) of the Prison Act. This is for possession or use of items which are prohibited under sections 40B, 40C and 40D of the Prison Act.
- 4.3.4 Further information and examples of when a central or local authorisation is needed can be found in Guidance Table on Central/Local Authorisations (Annex F).

Central (National) authorisations

- 4.3.5 Central S40B/E authorisation are already provided to several individuals and groups for specific purposes on behalf of the Secretary of State. Security departments are to maintain a local record of central authorisations. Security and gate staff should be aware of any central authorisations surrounding approved conveyance. A national central authorisations list can be requested via security.procedures@justice.gov.uk or be accessed via the National Security Framework digital page.
- 4.3.6 Central authorisations do not over-ride reasonable local rules and restrictions set down in an individual prisons' LSS concerning the conveyance and possession of a wider range of items, but any restrictions applied must be reasonable in the circumstances. For example, it would not normally be appropriate to routinely restrict locally, the conveyance of the following items without justification:
- Books.
 - Legal correspondence and paperwork.
 - Items for transgender individuals.
 - Items to assist disabled prisoners.
 - Prescribed medication.
 - Liquids and food.
 - Baby food.
 - Food brought in by approved ministers of religion for religious festivals if this cannot be provided by the prison. The bringing in of such food should always be agreed in advance by the prison.
- 4.3.7 Wearable technology (fitness trackers and smartwatches) is prohibited in prisons and all applications for wearable technology must be agreed locally prior to a central authorisation submission and not over-ride any local rules. Existing and future authorisations are to be reviewed after twelve months of issue.

OFFICIAL

- 4.3.8 A central authorisation will be granted for 12 months from the date of the authorisation, unless otherwise specified. After 12 months a local review should take place to establish whether the authorisation is still required and if so, an extension be requested from security.procedures@justice.gov.uk.

Local authorisations/Local lists

- 4.3.9 Governors/PGDs must ensure that any legitimate activity which has not been authorised centrally is covered by the issuing of a local authorisation. The use of a 'local list' of authorisations related to specific duties of staff must be considered. Guidance Table on Central/Local Authorisations (Annex F) lists examples where this may be appropriate and highlights which staff and items may be covered by Crown Immunity.
- 4.3.10 Governors must consider local restrictions set out in the LSS against the provisions of the Prison Act to ensure that they are comprehensive, clear, and appropriate, and must ensure that local lists of unauthorised items take into account items set out in Sections 40A to 40F of the Prison Act. Contravention of local lists/regulations will not be a criminal offence unless there is also contravention of the Prison Act.
- 4.3.11 Local authorisations considered by Governors or by gaining agreement from the PGD must be documented and the process set out in the LSS (see Template Form - Local Authorisation of Items, Annex B). These authorisations must be made locally by Governors for their individual prisons or where considered appropriate in the case of higher risk items, by the PGD on behalf of the Secretary of State. The LSS must specify how often the authorisations will be reviewed.
- 4.3.12 There are circumstances where it is necessary for persons in prison, including prisoners, to have possession of articles which, in another context, may constitute an offence under Section 40CA of the Prison Act. This includes knives, tools, religious artefacts (kirpan) and bladed items necessary for legitimate use. Authorisations must be in place to ensure that those in possession of such items for legitimate purposes are not committing a Crown offence if Crown immunity does not apply. Governors or authorised prison staff must issue local authorisations for any other reason prisoners or staff may need to possess such items.

4.4 Management of Conveyance via the Gate (see Guidance 6.3 for supporting information)

- 4.4.1 The main gate is a focal point for conveyance and can be vulnerable to conveyance of illicit items via individuals (staff, visitors, and official visitors) and vehicles.
- 4.4.2 Governors must undertake an evidence-based assessment (see Guidance 6.1) to identify the risk of conveyance and set out within the LSS agreed processes and searching procedures to be carried out on individuals, vehicles, and materials through the main gate. Procedures within the LSS for the secure entry and exit of every person, vehicle and item through the gate must be effectively communicated to gate staff.
- 4.4.3 The LSS must reflect the individual circumstances of the prison. All prisons, including those in the high security estate, must ensure that searching requirements within the LSS are also reflected in their Local Searching Policy for prisoners, staff, and visitors upon entry/exit of the gate. See the [Searching Policy Framework](#) for more information and guidance on Local Searching Policies.

OFFICIAL

- 4.4.4 Where a prison has more than one gate, these instructions apply to all gates, regardless of the nature of operations/function of the gate (e.g., delivery gate only). The specific risks posed by the operation of multiple gates must be considered in the LSS.
- 4.4.5 Rules 35A, 41, 64, 70, 70A, 71, 73 & 79 of the [Prison Rules 1999](#), Rules 11, 46, 69, 74, 74a, 75, 77 & 83 of [The Young Offender Institution Rules 2000](#) and sections 8, 8A & 40A-40F of the [Prison Act 1952](#) must be complied with when conducting the gate activities described in this Policy Framework.
- 4.4.6 In accordance with the provisions of the S19(1) of the Prison Act 1952, Prison Rule 79(2), YOI rule 77(2), S20 and S48 of the Health and Safety at Work Act 1974 and S54 of the Food Act 1990, the following people have a statutory right to enter a prison at any time:
- Justices of the Peace for the County or Borough of the prison or the prisoner in question.
 - Members of the prison's Independent Monitoring Board.
 - Health & Safety Inspectors of the Health and Safety Executive (HSE) enforcing Health & Safety legislation.
 - Local Authority Environmental Health Officers enforcing the 1990 Food Act or Food Safety (General Food Hygiene) Regulations 1995; and
 - Members of the European Committee for the Prevention of Torture.
- 4.4.7 Identities must be checked, and they may be searched subject to local requirements. Any searching must be in accordance with the [Searching Policy Framework](#).
- 4.4.8 Governors must ensure all individuals coming into a prison are aware of the items not permitted. They must be made aware that it is a criminal offence to convey into a prison and/or use certain items within a prison when Crown immunity does not apply, together with the associated penalties. Model notices are provided in Template Notice – Criminal Acts of Conveyance (Annex C) and Template Notice – Consequences of Conveyance (Annex D).
- 4.4.9 Governors must provide the use of appropriate storage facilities for staff, official visitors and visitors who use public transport to secure prohibited items such as mobile phones. Mobile phones and any other unauthorised items must not be stored within any lockers that are located past the searching process and beyond the confinements of the gate. Prisons that don't have the physical capacity due to their unique layout to provide storage facilities for staff travelling on public transport must gain authorisation from the PGD for staff to bring mobile phones into the prison up to the point where lockers are positioned.
- 4.4.10 Gate staff are critical to managing the risk of conveyance and improving detection or deterrence of any potential criminal activity. The duties of such staff must include:
- Identifying, controlling, and recording the authorised entry and exit of prisoners, people, vehicles, and materials/tools.
 - Ensuring that searching procedures, where applicable are carried out for individuals, vehicles, and materials in line with the LSS.
- 4.4.11 As a minimum, Governors must ensure that gate staff:
- Check the identification of all people entering the prison.
 - Record their names of delivery drivers and passengers.
 - Record the registration numbers of all vehicles entering/leaving the prison.
 - Record the time of arrival/departure of vehicles and visitors entering/leaving the prison.
 - Record in detail the next scheduled destination of vehicles.

OFFICIAL

- Allow only authorised people, items, and vehicles in/out of the gate (the items which are not permitted are set out in List A, B and C items (Annex A) in addition to any local lists).
- Record items leaving or being delivered to the gate.

4.4.12 Governors must undertake a risk assessment to set out arrangements for staff searching in accordance with [Searching Policy Framework](#).

4.4.13 Staff working in the gate must be aware of their role in local contingency plans for all types of incidents.

Vehicles

4.4.14 Governors must ensure that there is an effective process in place in the gate to provide assurance that staff are following the searching procedures set out in the LSS for both drivers and vehicles.

Vehicles entering

4.4.15 Governors must ensure that staff working in the gate and those escorting vehicles have access to a copy of the published prison procedures (core day).

4.4.16 Gate staff must be made aware of all relevant centrally issued authorisations and any local authorisations that allow list A, B or C items into the prison. Local authorisations must be recorded by the Security Department. See Template Form - Local Authorisation of Items (Annex B).

4.4.17 Any surplus equipment in the vehicle (such as rope and tools) that is not required in the prison must be secured at the gate and only returned to the vehicle when it is leaving.

4.4.18 Where vehicles contain built in cameras, the relevant person has a central authorisation in respect of Section 40C of the Prison Act 1952. Where such camera systems transmit footage electronically in real time to a central server, the relevant person has a central authorisation in respect of Section 40D(1)(b) and Section 40D(3A) of the Prison Act 1952. Where possible, the camera is to be switched off or covered by the driver prior to entering the prison. Where this is not possible, the relevant person has a central authorisation under Sections 40D(1)(a) and 40D (3) of the Prison Act 1952.

Emergency Vehicles

4.4.19 There is a central authorisation in place for ambulance staff to enter the prison with their work and personal devices (including personal mobile phones). Governors must ensure there are clear instructions within the LSS about the admission of emergency vehicles and that internal escorts for emergency vehicles are available. The instructions must be in accordance with the [Health and Safety Arrangements for the Management of Workplace Transport Policy Framework](#) and include:

- Clearing the gate area of any vehicles.
- Procedures for gate staff in respect of any searching requirements.
- Procedures for gate staff in respect of any central or local authorisations.
- Process for identifying a vehicle escort and any additional gate staff to assist with opening of gates on route to the incident area.
- Process for escorting emergency vehicles during prisoner movement.

OFFICIAL

- 4.4.20 The preservation of life must always take precedence over local procedures in any life-threatening situation. Arrangements must be in place for the processing and holding of delivery vehicles that may enter unsearched when permitting entry of an emergency vehicle through the vehicle lock. The delivery vehicle should be held in an area that is secure and prevents further movement. If a secure area is not available, a member of staff must remain with vehicle until it is searched.
- 4.4.21 Gate staff must ensure ambulance staff lock any personal mobile phones not for clinical use in secure lockers within the ambulance itself, where available or leave them in the glove box and never on display or taken to the scene. The prison must outline the process for accounting of personal devices entering and leaving the prison within the LSS.

Vehicle exiting

- 4.4.22 When the vehicle has completed the delivery and is ready to leave, the vehicle must be searched on exit in accordance with the [Searching Policy Framework](#) to make sure nothing is being conveyed out of the prison. Any searching to be conducted on the driver and passengers is to be determined locally following a risk assessment. Details must also be checked against the information provided on entry.

Vehicle searching and supervision

- 4.4.23 Governors must undertake an evidence-based assessment and set out in the LSS the process for searching vehicles (including any content, where applicable) on entry and exit, and the level of searching to be conducted on the driver and any passengers. Searching procedures set out in the [Searching Policy Framework](#) must be applied when searching. Vehicles not requiring a search on entry or exit, including the driver and any passengers, must be identified via a risk assessment, and documented in the LSS (see Guidance 6.1).
- 4.4.24 Staff must be provided with adequate searching equipment for the search of vehicles. See [Searching Policy Framework](#) for details on vehicle searching equipment.
- 4.4.25 Governors must ensure that if delivery items are to be decanted at the gate, the process is agreed locally and outlined within the LSS to include the agreed levels of searching and supervision relevant to the prison.
- 4.4.26 Governors must ensure that if delivery items are escorted through and decanted within the prison, the same level of searching and supervision is employed as when delivery items are decanted at the gate. This applies to all activity areas / workshops within the prison. If deliveries are unloaded by prisoners (kitchen for example) within the prison, then this must be supervised by staff. This process must be documented in the LSS. See Guidance on Workshop Deliveries (Annex J).
- 4.4.27 If staff have concerns regarding an upcoming or previous delivery, they must submit an Intelligence Report (IR).

Vehicle movement

- 4.4.28 Governors must ensure that the movement of all vehicles in the prison is only done with prior knowledge and/or authorisation of the communication/control room. The LSS needs to set out how movements into and around the prison will be managed by the communications/control room and the gate.
- 4.4.29 Governors must set out in the LSS which vehicles do not require an escort within the prison (not including the High Security Estate). An evidence-based risk assessment must be used

OFFICIAL

to determine the risks. This must be completed in conjunction with the Transport Risk Assessment as described in [Health and Safety Arrangements for the Management of Workplace Transport Policy Framework \(Annex A\)](#). Prior authorisation for unescorted vehicles to enter must be granted from the communications/control room.

- 4.4.30 Vehicles identified as requiring an escort within the prison must not be allowed to enter until escorting staff are available. It is the responsibility of the vehicle escort to always remain with the vehicle and never leave it unattended. Whilst escorting the vehicle to its location, staff must ensure the vehicle remains in sight. Local safe systems of work which comply with the requirements of [Health and Safety Arrangements for the Management of Workplace Transport Policy Framework](#) must be available to staff involved in supervising the movements of vehicles.
- 4.4.31 Unescorted vehicles and their occupants, when present in the prison must be confined to movement only in areas which prisoners cannot access, unless in circumstances where the prisoners are escorted or when a risk assessment determines otherwise.
- 4.4.32 The responsibility to control and monitor the vehicles of visitors/contractors extends to the prison's own vehicles.

Training

- 4.4.33 All staff undertaking vehicle escorts must be trained to a competent level and be aware of the location and appropriate use of personal safety equipment clothing and methods of communication with the driver during the escort. A training programme for vehicle escorts and trainers is provided through Learning and Development. See [Health and Safety Arrangements for the Management of Workplace Transport Policy Framework](#) for further information.

Staff Vetting

- 4.4.34 Governors must adhere to the requirements set out in [Security vetting: PSI 07/2014](#) and [Security vetting: additional risk criteria for ex-offenders, PSI 27/2014](#). There must be clear local arrangements for adhering to vetting set out in the LSS.
- 4.4.35 The level of security clearance varies according to the security category of the prison and the role of the person entering the prison. Governors must ensure that before being granted access to the prison to work, all Directly Employed (DE) and non-Directly Employed (NDE) staff have acquired the appropriate security clearance for the prison and their specific role. Professional or Official Visitors who do not work for us in either capacity and do not go through our security vetting must be deemed as appropriate by the Governor to enter.

Corruption

- 4.4.36 HMPPS defines corruption as a person in a position of authority or trust who abuses their position for benefit or gain for themselves or for another person. Governors must ensure that all staff (including non-directly employed) are aware of the responsibilities outlined in the [Counter Corruption and Reporting Wrongdoing Policy Framework](#).

Enhanced Gate Security Measures (see Guidance 6.3 for further information)

- 4.4.37 For those prisons with Enhanced Gate Security (EGS), these measures (X-ray baggage scanner and archway detector) when used effectively alongside handheld metal detectors and physical searches can support in the detection and reduction of illicit items being conveyed into a prison. Prisons can also utilise the trace detection equipment in the gate. See [Use of drug trace detection equipment in prisons Policy Framework](#).

OFFICIAL

- 4.4.38 The security procedures of EGS must be included within the LSS and prison's Local Searching Policy.
- 4.4.39 The expectation is that all visitors and staff entering the prison will be subject to enhanced gate search procedures and searched in line with local LSS arrangements and [Searching Policy Framework](#).
- 4.4.40 Signage laying out the penalties for the conveyance of prohibited items in/out of prison must be present in both the gate and internal areas of the prison (see Template Notice – Criminal Acts of Conveyance Annex C and Template Notice – Consequences of Conveyance Annex D). Where possible audio and visual warnings should also be in use.
- 4.4.41 EGS prisons must aim to run 100% gate searching at all times. In exceptional circumstances staff may be deployed for security tasks for a limit period, for example where a prison needs to respond dynamically to threat displacement (e.g., supply via a different conveyance route), prisons may deploy staff away from the gate for a limited period. The objective should be to restore to 100% searching as soon as operationally viable. Where there are insufficient staff available to enable 100% searching, the objective should be the highest percentage of searching possible, managed according to risk and in agreement with the PGD. Searching must not commence until the gate is staffed for searching.
- 4.4.42 After completing identity (ID) verification, all persons entering the prison via the gate must be asked by a member of the searching staff if they have any unauthorised items on their person before commencing the mandatory search process.
- 4.4.43 The searching process must include the following:
- Collect a tray, empty pockets, remove all metallic objects, such as jewellery, watches, belts, and outer clothing, e.g., coats/jackets, and place items flat into the tray and not on top of each other.
 - Food and drink must pass through the X-ray Baggage machine. Drinks must be in a factory sealed bottle to enter the X-ray Baggage Scanner or an empty bottle. This will prevent any spillage on to the X-ray Baggage Scanner. Unsealed bottles and hot drink cups must not enter the X-ray Baggage Scanner.
 - Search all personal belongings using the X-ray baggage machine.
 - X-ray baggage scanner to be always operated by two members of trained staff, one for the operation of the X-ray Baggage Scanner and the second to assist with any manual searching of items/property.
 - If a trained member of staff suspects the belongings may contain an illicit item, they must highlight the item for a visual search by staff.
 - If X-ray baggage scanner staff suspect they have discovered an explosive device or any individual components that would be required to build an explosive, they must instruct another trained member of staff look through the images to confirm what they have seen. Advice will then need to be sought from a manager immediately. See [Improvised Explosive Devices Policy Framework \(Restricted\)](#) for further information.
 - Some prisons may choose to undertake a secondary search of personal belongings based on risk. If an individual refuses the search of their personal belongings, the duty governor will determine the most suitable way forward.
 - If any individual refuses a search, including staff, the Duty Governor will decide if they are to be refused entry and subjected to a conduct and discipline investigation. However, in some instances, the staff member will be detained and subject to arrest under the [Police and Criminal Evidence Act 1984](#) (PACE).

OFFICIAL

- All persons will walk through the archway metal detector and follow instructions given by the operator.
- If the alarm sounds, the operator will ask the person to account for the alarm. If items are removable, they must be put through the X-ray baggage scanner.
- The person will then be subjected to the handheld metal detector, followed by a rub down search. See [Searching Policy Framework](#) for guidance on use of hand-held metal detector wands during a search.
- If the archway metal detector alarms at the feet, shoes must be removed and X-rayed on every occasion.
- The person will then be subjected to the handheld metal detector, followed by a rub down search.
- Boots with steel toe caps are likely to cause the archway to alarm, to speed up the process through EGS, it is recommended these are removed prior to the person passing through the archway metal detector.

- 4.4.44 All alarms must be explored, and the source of the alarm must be identified wherever possible. If an item is identified and can be removed, it must be put through the X-Ray baggage scanner and the person must be subjected to the handheld detector and a rub down search to ensure no other metal is present. If the metal cannot be removed (for example, due to internal plates/pins, underwired bra or a disability that requires the use of aids that contain metal etc.) and the person is able to declare why the alarm has activated, the person must be subject to a rub-down search and use of the hand-held metal detector to identify the potential item and to ensure no other metal is present.
- 4.4.45 The random percentage of staff to be rub-down searched must be set out in the LSS for each prison. As a minimum, this must be at least 10% of all staff entering the prison daily. The recommendation is to utilise the random selection system built in the archway metal detector. If the archway metal detector activates and displays QUOT, the machine has identified the person for a random search and is an indication there's no metal present on the person. The person is to receive a rubdown search and there is no requirement to use a handheld metal detector. The LSS must outline the process which the prison will use in selecting individuals to receive a random rub down search.
- 4.4.46 All visitors will be subject to a rub-down search and place items through the X-ray baggage scanner on every occasion in line with the requirements of the [Searching Policy Framework](#).
- 4.4.47 The search of visitors and staff by search dogs must be in line with [Prison Dogs Policy Framework](#) which provides further instruction on using search dogs and describes what staff must do when a passive search dog provides an indication.
- 4.4.48 Prisons must have dog handler support in place to deliver the highest level of search on visitors and staff, according to risk.

Searching staff and visitor's bags/belongings in the absence of an X-ray baggage scanner

- 4.4.49 If the X-ray baggage scanner is unable to be used (i.e. where two trained staff are not available), the searching of staff must follow the process below:
- Staff must empty their pockets, remove outer clothing, and empty food, drink, and keys from their bag into the tray provided at the gate.
 - A member of gate staff will examine the contents emptied into the tray and provide an examination of the items remaining in the bag. This examination will involve checking all areas of the bag, including pockets, for non-authorized items.
 - Staff will walk through the archway metal detector and follow the process outlined at 4.4.43 if the warning light or alarm sounds.

OFFICIAL

4.4.50 A randomised process must be in place for a percentage of staff bags to receive a secondary, physical search by a member of gate staff. This will be in local policy and will explain how the process is truly random and documented in the LSS.

4.4.51 All visitors will have their bags examined via a search following the same process outlined in 4.4.49. The process for visitors bringing bags and specific items into the prison will be captured in each prison's LSS and this must be adhered to. All visitors will also be subject to walking through the archway metal detector and a rub-down search.

Dealing with suspicious items and unauthorised finds

4.4.52 In the event of someone refusing to open their bag, staff must inform the Security Manager/Orderly Officer. A member of the searching team should have access to a radio to facilitate this contact.

4.4.53 In accordance with [Searching Policy Framework](#), local arrangements must be in place to investigate and deal with suspicious items identified by the X-ray process. This may involve asking the person to open the bag or item themselves to explore the source of the suspicion or asking the owner for permission for gate staff to do so in the presence of the owner. If a person refuses, this must be escalated to a Security Manager/Orderly Officer and the person may be refused entry to the prison. If the person does leave the prison, it is good practice to record this on the intelligence system. [Searching Policy Framework](#) states that a bag may be forcibly searched where there is reasonable suspicion that it contains illicit items. See [Improvised Explosive Devices Policy Framework \(Restricted\)](#) for actions following the discovery of a suspected explosive device or components.

4.4.54 Prisons can also utilise the trace detection equipment in the gate. See [Use of drug trace detection equipment in prisons Policy Framework](#).

4.4.55 Illicit items found during a search must be dealt with in accordance with [Management and Handling of Evidence Policy Framework](#) and an IR submitted.

4.4.56 The prison must consider whether the case should be referred to the police in accordance with the [Crime in Prison Referral Agreement](#).

Pacemakers and implantable cardioverter defibrillators (ICDs) searching restrictions

4.4.57 A person wearing a pacemaker may be subject to a search using a metal detector portal or handheld detector. Being too close to a magnetometer could result in a pacemaker switching to magnet mode where the pacemaker simply paces the heart at a flat pre-programmed rate rather than the patient's heart rhythm. For ICD devices, the consequences can be very serious delivering painful high voltage shock therapy at a time when it is not needed. HMPPS devices transmit a low electromagnetic field but searching must be in accordance with the below conditions.

- Metal Detector Portal Search:
 - If a person informs staff, they that have a pacemaker or ICD inserted and/or presents a cardiac device ID, they must be asked to walk quickly through the system. They should not stop or linger in the archway.
- Handheld Metal Detector Search:
 - British Heart Foundation guidelines state that people with pacemakers can be searched with this equipment, however the device should be held at a minimum distance of 15cm. Staff must not hold handheld wands over heart devices or wave them back and forth over the area where the device is fitted (most heart devices are located next to the collar bone, but they can be positioned

OFFICIAL

elsewhere on the torso). Exposure to screening wands should be limited and staff should only pass the wands very quickly over the device whilst, maintaining the safety distance.

- People with an ICD fitted may be exempted from searches using a handheld metal detector. If a handheld metal detector is held over an ICD for too long, the consequences can be very serious. Staff must be trained in the procedure for its use, where prisons require all staff to be searched using a handheld metal detector or where there is intelligence or reasonable suspicion that requires its use.

Radiation safety

- 4.4.58 To comply with [The Ionising Radiations Regulations 2017](#) (IRR17), HMPPS has a contract with a radiological service provider to deliver the Radiation Protection Advisor (RPA) services for radiation safety survey inspections and Radiation Protection Supervisor (RPS) training and local radiation advice. Private prisons must appoint an RPA. These services are a legal requirement for HMPPS to operate X-ray equipment and must be undertaken. See [PSI 18/2015 Health and Safety Arrangements for Radiation Safety of X Ray Security Equipment](#) for the responsibilities of an RPA.
- 4.4.59 Governors must appoint a competent and trained member of staff as the RPS for each area of the prison where an X-ray scanner, such as the X-ray baggage scanner, is used. Refer to [PSI 18/2015 Health and Safety Arrangements for Radiation Safety of X Ray Security Equipment](#) for comprehensive instructions relating to the RPS role.
- 4.4.60 RPA services are only required for the X-ray equipment i.e., baggage scanner and body scanner.
- 4.4.61 The RPA must carry out a radiation safety survey inspection(s) of the X-ray baggage scanner as part of their visits to ensure that the machine is not operating outside of the authorised parameters and the equipment specification. These radiation safety survey inspection(s) will be undertaken:
- i. annually.
 - ii. if the equipment is re-located; or
 - iii. following the replacement of any component that directly affects radiation exposure.
- 4.4.62 The RPS must ensure that the radiation operation is controlled in accordance with local rules and compliant with legislative requirements identified by the RPA. The RPS must undertake a weekly safety check of the X-ray baggage scanner equipment and record the results in the RPA radiation protection book.

Installation/Re-location of equipment

- 4.4.63 Contracted prisons must ensure that the Health and Safety Executive (HSE) is notified of any ionising radiation equipment and its use. If in doubt to the HSE registration status, contracted prisons should seek the advice of their appointed RPA regarding the requirements for HSE registration. Individual notification for public sector prisons is not required as this is undertaken centrally by the MOJ.
- 4.4.64 Archway metal detector installations must be undertaken by a competent installer, who is typically the supplier. Once installed, archway metal detectors must not be moved. If it becomes necessary to relocate the archway metal detector, a further assessment is required and must be completed by an approved installer/contractor.

OFFICIAL

- 4.4.65 In accordance with [PSI 18/2015 Health and Safety Arrangements for Radiation Safety of X Ray Security Equipment](#), when new X-ray equipment (X-Ray baggage scanner) is installed or existing equipment is moved to a new location, Governors and the head of security must ensure that a critical examination is carried out by the installer before the equipment goes into use. The supplier will undertake a critical examination to ensure that:
- i. the safety features and warning systems operate correctly; and
 - ii. the equipment provides sufficient protection for all persons against exposure to radiation.
- 4.4.66 The supplier shall provide a written report on the outcome of the critical examination together with adequate information about the proper use, testing and maintenance of the X-ray baggage scanner. The local RPS must ensure this report is kept in the RPA radiation protection book and that any recommended requirements are undertaken during the daily operator and weekly RPS checks.

Maintenance/Serviceing

- 4.4.67 The Governor has ultimate responsibility for ensuring that equipment is maintained in accordance with the manufacturer's recommended maintenance schedule and technical specification. Contracted prisons must seek the advice of their appointed RPA regarding requirements for maintenance.
- 4.4.68 Written maintenance/service reports for the X-ray baggage scanner and archway metal detectors will be held in the Security Department. The RPS must ensure copies of these reports are kept in the RPA radiation protection book. This includes certification/re-certification of the mandatory verification of the calibration of the archway metal detector.
- 4.4.69 Prisons must consider adding EGS equipment to a central HMPPS prison asset register. This will ensure all equipment is inspected/maintained and easily located during the RPA visit. Equipment provided as part of the Security Investment Programme (SIP) falls under a central maintenance contract and any work to be undertaken must be in accordance with central contracts.

External maintenance

- 4.4.70 To maintain archway metal detections as per the manufacturer guidance and facilities management best practice, the service provider must carry out annual preventative maintenance visits. The first year planned preventative maintenance (PPM) is included in the purchase price of the unit and must be conducted on or before the anniversary of installation. After this point, prisons must raise their own Purchase Orders for annual maintenance. SIP assets will be provided with PPM visits centrally in accordance with the agreed arrangements.
- 4.4.71 Beyond the Portable Appliance Test (PAT), there is no formal external maintenance required of hand-held metal detector wands since this goes against the manufacturer's advice as the equipment has no moving parts to maintain. Operators of the wand must undertake a pre-user check, look for any damage and battery discharge prior to use and check with metal items to ensure they detect.
- 4.4.72 Supplier checks be carried out on the X-ray baggage scanners in line with agreed arrangements. Local arrangements must be undertaken for annual checks of X-ray baggage scanners that have purchased outside of SIP.

OFFICIAL

4.4.73 The RPA is responsible for visiting each prison annually where X-ray equipment is installed. These visits will include an inspection and survey of X-ray security equipment and reviews of radiation safety.

Assessments

4.4.74 In accordance with the [Ionising Radiations Regulations 2017](#) before equipment is put into use every prison must undergo an initial Ionising radiation risk assessment of the potential risk of exposure to radiation for staff operating the machines. The assessment identifies all hazards with the potential to cause radiation. The Governor must ensure that any measures identified by the ionising radiation risk assessment, as being required to restrict exposure, must be implemented.

Prison owned assessments

4.4.75 In accordance with [PSI 37/2015 Health and Safety Arrangements for Risk Assessment](#), the manager (Head of Function) should lead the risk assessment process and retains the responsibility to ensure the completed assessment is suitable and sufficient.

4.4.76 The Head of Function responsible for the risk assessment must ensure control measures identified are implemented and followed. Where additional control measures are identified to reduce the level of risk associated with a hazard these must be completed within the timescale specified by the risk assessment document.

4.4.77 The Head of Function, responsible for the X-ray baggage scanner in the prison, must ensure that the ionising radiation risk assessment is undertaken before the X-ray baggage scanner machine is first used and updated whenever there is a change in practice, following relocation or an accident. See Ionising Radiation Assessment (Annex E1).

Prison owned machinery checks (see Enhanced Gate Security - Summary of Equipment Checks Annex E2)

4.4.78 Running performance test pieces through both the metal detection and X-ray equipment is the responsibility of the Security/Operations Department and a critical assurance activity that supports to understand how the kit is performing. It is also the Security/Operations Department's responsibility to oversee and review the operator's capability to find illicit/unauthorised items using these search aids effectively and efficiently and to offer support and guidance as required.

4.4.79 X-ray baggage scanners, archway metal detectors and hand-held metal detector wands are covered under the standard PAT, which must be carried out across all prisons for all electrical items fitted with a standard plug top. If the equipment is wired directly into a fused spur the equipment does not require PAT testing. The PAT is carried out by the facilities management provider every 12 months. In terms of the hand-held metal detector wand, the wand charger is tested rather than the wand itself as they are battery-operated.

4.4.80 The X-ray baggage scanner operator must undertake a daily safety check before the machine is used. This must include ensuring that the warning light and emergency stop are working correctly and any other recommended manufacturer or engineer requirements. The daily check will be carried out by those staff who are trained in operating the X-ray baggage scanner. There must be a signed record of these checks kept with the X-ray baggage scanner and keep these records in the RPA radiation protection book. The EGS Manager should assure themselves that these checks are being completed. The RPS is responsible for undertaking the IRR17 mandated safety checks.

OFFICIAL

- 4.4.81 X-ray baggage scanners must also undergo weekly checks by the operator to assess whether the unit is working at optimum performance. These weekly checks will be made known during the 'X-Ray Baggage Scanner' training course by Learning and Development. The weekly check will be carried out by those who are trained in operating the X-ray baggage scanner.
- 4.4.82 Archway metal detectors must undergo weekly checks by the operator. This involves conducting a walk test through the archway using a performance test piece for the HMPPS programmed setting (small/medium/large object), plus a phone test piece for the ferromagnetic detection. There must be a local record of these checks.

Training

- 4.4.83 All staff who are deployed to searching at the gate must receive local searching refresher training annually. The training can be delivered locally by appropriate staff, but training records must be made available for audit purposes.
- 4.4.84 Governors must ensure that all staff who are deployed to searching tasks involving the X-Ray baggage scanner have completed the 45-minute e-learning and have received the mandatory 'X-Ray baggage scanner' training provided by Learning and Development. Staff working on the X-ray baggage scanner must be annually assessed by the RPS as competent in the use of this equipment. A record of trained operators and their annual competency check must be kept in the RPA radiation protection book.
- 4.4.85 Staff who are deployed to searching at the gate and managers with oversight of that area must complete local training on the use of the archway metal detector and handheld metal detector. Staff must be annually assessed by a manager as competent in the use of this equipment. There must be a local record of who has undertaken the training and the annual competency check.
- 4.4.86 Staff deployed to searching at the gate must be offered the 'Back to Basics Foundation Course' delivered by Learning and Development. This course discusses theory and knowledge relating to archway metal detector use only. It does not include operation of the equipment hence the need to have received local operator training delivered by local staff, in advance of the 'Back to Basics Foundation Course'.
- 4.4.87 The Governor must ensure that staff who undertake the RPS role complete the RPS training before they issue the RPS appointment confirmation. To receive a certificate evidencing completion of the training the staff member will have had to demonstrate sufficient knowledge and competency in radiation matters and have completed the full training course. The certificate must be kept in the RPA radiation protection book along with a copy of the RPS appointment letter. See Enhanced Gate Security - Radiation Protection Supervisor Appointment Letter (Annex E3)
- 4.4.88 RPS training (including refresher training) is coordinated by the Body Scanner Governance & Support team. RPSs must attend an RPS refresher training course every three to five years or when there is a change in practice or technology, and a training record must be held at each prison and on the national database via SOP. The original RPS certificate will need to be archived and replaced with the subsequent training certificate. Prisons should email bodyscannersupport@justice.gov.uk to book a place on an RPS training course.

Local rules for X-ray baggage scanners

- 4.4.89 In accordance with [Ionising Radiations Regulations 2017](#), work with ionising radiation must be carried out in accordance with written safety procedures, referred to as local rules. Local

OFFICIAL

rules are a set of instructions laying down how the work should be carried out to restrict exposure to radiation (and ensure compliance with relevant legislation). See Enhanced Gate Security - Baggage Scanner Local Rules (Annex E4) for a template.

- 4.4.90 In accordance with sections 18 and 19 of the [Ionising Radiations Regulations 2017](#) the Local Rules must also:
- Details of the RPS(s);
 - Description of any designated areas;
 - General operational procedures (which are pertinent to radiation safety);
 - Actions to be taken in the event of a radiation accident;
 - Dose investigation level.
- 4.4.91 In accordance with [PSI 18/2015 - NOMS Health and Safety Arrangements for Radiation Safety of X Ray Security Equipment](#), the RPS must ensure that adequate local rules are available and are being complied with by all staff and others who may come into contact with the X-ray equipment. The governor must ensure that a copy of the local rules is displayed in a clearly visible location near the machine. Staff trained in operating the X-ray baggage scanner must read the local rules annually and then sign a register, which will be held in the RPA radiation protection book, to confirm that they have read, understood, and will adhere to the local rules.

Procurement

- 4.4.92 Public sector prisons must not purchase X-ray baggage scanners or related equipment outside of the MOJ contract. The equipment has been tested and deemed fit for purpose. Privately managed prisons can purchase equipment outside of the contract.

Assurance

- 4.4.93 There is a central request for prisons to submit their EGS data for assurance purposes which must be submitted in a timely manner.
- 4.4.94 See Guidance 6.3 for further information and supporting tools on EGS.

4.5 Management of Conveyance via Prisoner Reception (see Guidance 6.4 for supporting information)

- 4.5.1 Governors must undertake an evidence-based assessment to identify the risk of conveyance in reception (see **Guidance 6.1**). Each prison has a unique reception area and different functions. This must be taken into consideration when undertaking the assessment of the risk including the availability of technical aids and staffing resources for searching.
- 4.5.2 Where conveyance via this route is an identified risk, where relevant to the prisoner, Governors must ensure that all necessary procedures for the safety of prisoner and the prison are put in place.
- 4.5.3 Reception procedures must follow the requirements set out in [PSI 07/2015 Early days in custody](#).
- 4.5.4 Governors must ensure that all staff working in reception are fully aware of conveyance risks. Risks linked to the pressures on prisoners being recalled to custody, and prisoners returning from category D prisons to convey illicit items must be identified and mitigated, where possible. See Support Links for Staff, Prisoners and Visitors (Annex X) for information support measures.

OFFICIAL

- 4.5.5 Governors must ensure that the LSS sets out the searching arrangements to manage the risk of conveyance when prisoners are arriving both inside and outside of the agreed opening hours to include during night state.
- 4.5.6 Governors must ensure that prisoner records that accompany each prisoner are reviewed in reception to identify any immediate risks of conveyance (specifically risks of drug/phone conveyance and concealment of weapons/other items). This applies to prisoners on initial reception and prisoners on transfer from another prison.
- 4.5.7 Governors must ensure that any security concerns in relation to a prisoner found to be conveying an illicit item during a police production is reported immediately to the Duty Governor.
- 4.5.8 Governors must ensure that all information in relation to conveyance, searching and use of technical aids is appropriately communicated to prisoners with protected characteristics, including those with physical or learning disabilities and those who do not speak English.

Reception searching

- 4.5.9 Governors must ensure that searching of all prisoners entering and leaving the prison is in line with [Searching Policy Framework](#) in respect of minimum searching requirements and that this is reflected in the LSS. See also [Use of X-ray body scanners \(adult male prisons\) Policy Framework](#).
- 4.5.10 Governors must ensure that all prisoner property processed via reception is searched in accordance with the [Searching Policy Framework](#). Governors must ensure that stored and delivered property from prisons is, as a minimum, to be seal checked. Additional searching procedures must reflect the current conveyance risk and documented in the LSS.
- 4.5.11 Governors must manage property which has been confiscated as a result of it being illicitly conveyed into a prison in accordance with [Prisoners' Property Policy Framework](#). Any item collected as evidence must be preserved and managed in accordance with the Management and Handling of Evidence Policy Framework.
- 4.5.12 Governors must determine whether a programme of routine area searching in reception is required in addition to intelligence led-searching and based on a risk assessment, see [Searching Policy Framework](#). If the need for routine area searches is identified, this must be documented in the LSS including the frequency and to what depth.
- 4.5.13 Governors must ensure that decisions on how to safely manage the location of prisoners found in possession of an illicit item during a reception process are communicated to all staff, recorded on NOMIS and an IR submitted. This is particularly relevant when bullying/coercion is a factor in conveyance.

4.6 Management of Conveyance via Correspondence (see Guidance 6.5 for supporting information)

- 4.6.1 Prisoner correspondence is used by some individuals as a means of conveying illicit items into prisons. Governors must undertake an evidence-based assessment to identify the risk of conveyance posed by correspondence and ensure effective procedures are put in place and outlined in the LSS, taking into consideration the category of the prison, previous intelligence and finds of illicit items within the mail (see Guidance 6.1).
- 4.6.2 Governors must set out in the LSS the process for managing all correspondence received into the prison (to include legal, confidential and staff correspondence). Any procedures

OFFICIAL

must be lawful and in accordance with [PSI 49/2011 Prisoner communications policy](#) and [Authorised Communications Controls and Interception Policy Framework](#).

- 4.6.3 Whilst it is recognised that legal and confidential correspondence is one method where prisoners may receive illicit items, prisons must not introduce processes that treat all such correspondence as suspicious, without justification.
- 4.6.4 The Governor must ensure all mail including staff mail is received, processed, and checked in one location, for example the mail room before being moved on to other areas.
- 4.6.5 Any documents provided to a prisoner during a legal visit must follow the same process as legal correspondence being sent into the prison.

4.7 Management of Conveyance via the Perimeter (see Guidance 6.6 for supporting information)

- 4.7.1 The prison perimeter is used by some individuals as a means of conveying illicit items into prisons which can be a significant security threat. Governors must undertake an evidence-based risk assessment to identify the risk of conveyance posed by the perimeter. See Guidance 6.1.
- 4.7.2 Governors must set out in the LSS the process in place for managing conveyance via the perimeter. Actions to be put in place must be in line with the [Prison dogs Policy Framework](#), [Searching Policy Framework](#) and [Use of CCTV \(Overt Closed-Circuit Television system\) Policy Framework](#).
- 4.7.3 Governors must be alert to the risks posed to prisoners who receive items as a result of items being conveyed via the perimeter. Prisoners can enter into debt which can result in violence, self-harm, and suicide.

Perimeter searching

- 4.7.4 The LSS must outline the perimeter security applicable to the prison, together with the measures to ensure that levels of security are maintained and remain effective. This includes the processes in place, including the frequency of patrols, and method of searching applicable, based on risk.
- 4.7.5 Governors must ensure that perimeter checks are completed in line with the procedures outlined in the [Searching Policy Framework](#).
- 4.7.6 Governors must ensure that external and internal perimeter checks are coordinated by the control/communications room and recorded in the communications room log. This process must be set out in the LSS.
- 4.7.7 Netting and anti-drone technology are used for perimeter security, this must be controlled, monitored, tested, and comply with the MOJ technical standards specification.
- 4.7.8 Any use of CCTV to monitor activity around the perimeter must only be for professional and official purposes. The data and imagery captured and/or recorded on any system must be managed, stored, or deleted in accordance with the [Use of CCTV \(Overt Closed-Circuit Television system\) Policy Framework](#).

Control/Communications rooms

- 4.7.9 The use of an effective communications network to alert to possible conveyance risks can be a valuable mitigation. For the effective use of the radio in prisons, the following is required:
- All radio users are trained in the secure handling of the radios.
 - When drawing a radio staff must ensure that it is in full working order with sufficient battery.
 - A record of the identities of all out-stations is known by control/communications.
 - Regular net test calls/safety polls are carried out each day and any failures to respond are investigated and documented in the control/communications room log.
 - Each separate residential unit have at least one member of staff on duty who has drawn a radio and is logged onto the radio network.
- 4.7.10 The radio net must only be used for official purposes. All users must ensure that the network is used securely.
- 4.7.11 The role of staff working in the communications or control room in respect of conveyance is to:
- Control and authorise both routine and unscheduled movement of prisoners, staff, contractors, visitors, and vehicles within the prison.
 - Receive, evaluate, report and act upon information and indications of events.
 - Manage initial responses to events and emergencies.
 - Control and maintain the radio net and ensure secure usage.
 - Maintain secure practices and efficient operating procedures.
- 4.7.12 To achieve the above, Governors must ensure that staff working within the communication or control room have the required competence to handle, report and record information received via the radio, alarms, monitoring equipment, or any other source, as well as being conversant to the appropriate degree with the prisons intelligence system. It is recommended that all staff who work in the control room complete: [CRFE: Control Room for Future Operatives eLearning \(mydevelopment.org.uk\)](#) and the face-to-face Prison Radio Control Room Procedure course, particularly if working in the comms room alone
- 4.7.13 The LSS must set out the role to be played how communication or control room staff in managing conveyance via the perimeter, with particular emphasis on throw overs and drone activity.
- 4.7.14 Local communication instructions to quickly identify a conveyance perimeter threat may include actions such as seeking a response from specified outstations. This must be documented in the LSS.
- 4.7.15 The LSS must set out how communication and control room staff are to be kept informed of relevant information about incidents and, in line with the [Incident Management Policy Framework \(Restricted\)](#) they must have an up-to-date and working knowledge of the local contingency plans and be able to always maintain the security of the communication network.
- 4.7.16 Staff working in communications or control rooms must have access to local contingency plans in the event of an incident and be aware of their role. Local contingency plans, as required by the [Incident Management Policy Framework \(Restricted\)](#) must be provided outlining action to take following the positive indication of a conveyance threat to the perimeter, including reference to contingency plans where appropriate.

OFFICIAL

4.7.17 The LSS must include details of maintenance contracts and the communication or control room should keep a register of emergency call out numbers.

Internal movement

4.7.18 All internal movement of prisoners must be assessed locally as per the [Management of Internal Security Procedures \(Closed Prisons\)](#). The LSS must set out the agreed level of control and supervision provided to maintain security and safety in respect of conveyance. There must be clear guidance set out within the LSS regarding entry of prisoners to sterile areas and/or other areas where prisoners are not routinely permitted.

4.7.19 Security risks may dictate that additional security measures are put into place before a prisoner movement takes place. Such procedures must be based on an assessment of risk.

4.7.20 Prisoner movements that take place outside of main movement such as group or individual movement to activities must be controlled to ensure limited opportunity for prisoners to access illicit items that have entered the prison via the perimeter.

Exercise yards and external activity areas

4.7.21 Searching of exercise yards and external activity areas must be assessed locally and set out in the LSS, considering the risk of conveyance via the perimeter. This will also consider factors such as location to external perimeter and intelligence on conveyance routes. Searches of exercise yards must be in accordance with the [Searching Policy Framework](#).

4.7.22 Staff supervising activities in exercise yards, sports fields or other outside activity areas must draw a radio and join the network using the designated call sign. If staff supervising activities are working in an area beyond the range of the radio network, alternative means of communication need to be identified and managed.

Drone activity

4.7.23 Governors must ensure that the procedures in place to report and tackle drone activity are clearly detailed in the LSS.

4.7.24 Drone activity must be reported via an IR with and any seizures handled in accordance with the [Management and Handling of Evidence Policy Framework](#).

4.8 Management of Conveyance via Visits (see Guidance 6.7 for supporting information)

4.8.1 Visits are used by some individuals as a means of conveying illicit items into prisons. Governors must undertake an evidence-based assessment to identify the risk of conveyance via visits to inform local procedures (See Guidance 6.1). All procedures must be outlined in the LSS. Any searching requirements identified must adhere to the [Searching Policy Framework](#).

4.8.2 The LSS must include instructions to manage, supervise, and review any visits to prisoners, whilst also setting out security procedures to prevent passing of illicit items, this includes the searching of any toilet facilities. This includes prisons where visits may be held on units, during 'family days' and/or include overnight stays for mothers and families as per the [Pregnancy, MBUs and Maternal Separation in Women's Prisons Policy Framework](#).

4.8.3 All visitors must be made aware that conveying or depositing illicit items in any place in a prison, with the intent of coming into the possession of a prisoner is a criminal offence and informed of the responses and consequences of such actions. See Template Notice –

OFFICIAL

Criminal Acts of Conveyance (Annex C) and Template Notice – Consequences of Conveyance (Annex D). Governors must ensure that secure facilities are provided for visitors to store any items not permitted to enter the prison for the duration of the visit.

- 4.8.4 When searching visitors, consideration must always be made to preserve decency and dignity. Staff must search visitors respectfully, with due consideration to any cultural and religious diversity or disability. See [Searching Policy Framework](#).
- 4.8.5 Legal advisers are permitted to convey certain IT equipment into prisons. Only if there is a reasonable belief that this equipment is not for legitimate legal use can further restrictions be put in place. If there is a reasonable belief, and/or restrictions are put in place, an IR must be submitted to record this. See Guidance on IT Equipment Authorisation for Official Visitors (Annex U).
- 4.8.6 Powers to impose restrictions on visits and visitors are set out in [The Prison Rules 1999](#) Rules 34 and 73 ([The Young Offender Institution Rules 2000](#) Rules 9 and 77). See also [Management of Security at Visits Policy Framework \(Closed Prisons\)](#).
- 4.8.7 Governors must be alert to the fact that both visitors and prisoners involved in conveyance via visits may be vulnerable and under pressure to convey in this way.
- 4.8.8 The conveyance and/or possession of List A items into a prison must be reported to the police for investigation in line with the [Crime in Prison Referral Agreement](#).

4.9 Conveyance of Medication

- 4.9.1 The following people are authorised by the Secretary of State in accordance with Section 40B of the Prison Act for the following purposes:
- Delivery drivers conveying pharmacy, medical, veterinary, dental supplies into prisons where there is a valid order for those supplies from the prison to whom the delivery is being made. Also, delivery drivers conveying such items intended for delivery at another address, provided that there is no intention to bring those items out of the delivery vehicle whilst in prison grounds.
 - Staff who need to bring in controlled drugs as part of medication subject to them seeking agreement from the Governor/Director or their nominated representative to do so. This is on the condition that:
 - a) the controlled drug has been prescribed for their own use; and,
 - b) it is or may be necessary for them to take that drug whilst on prison premises for healthcare reasons; and,
 - c) they have followed any local rules and authorisations for bringing into prison such drugs.
 - Visitors to prisons who need to bring in controlled drugs as part of medication. This is subject to:
 - a) the controlled drug having been prescribed or legitimately purchased for their own use,
 - b) the visitor must declare the drug on entry and state that it is necessary for them to take that drug whilst on prison premises,
 - c) the prison must be satisfied that this is the case; and,
 - d) the visitor must follow any local rules and authorisations required for bringing into prison such drugs.
 - Emergency paramedic or ambulance or other emergency medical staff called to the prison conveying controlled medication.

OFFICIAL

- 4.9.2 The Head of Healthcare, Head of Security and lead pharmacist are required to work together in ensuring that instructions are documented in the LSS describing the procedures for access to the pharmacy and control of pharmacy keys both day and night. As a minimum this must include that the keys are held in a lockable safe and / or secure pouch. There must be an auditable record for the keys being taken out and returned. This may differ for those prisons with 24hr healthcare compared to those with healthcare throughout the core day only.
- 4.9.3 The LSS must set out a secure method of conveying drugs to areas and residential units which includes the method of dispensing them safely. Consideration must be given to:
- Times of day.
 - Routes to be taken.
 - Secure storage carriers.
- 4.9.4 Controlled drugs must always be kept in a locked cabinet in a secure room and any drugs to be disposed of must to be dealt with in accordance with legally required standards.
- 4.9.5 The prison pharmacist must comply with the requirements of [Healthcare for offenders](#).

4.10 Long Term High Security Estate and Restricted Status Prisoners

- 4.10.1 The policies relating to the Long Term High Security Estate, and Restricted Status prisoners contain mandatory requirements that may not be subject to local discretion. Directions about the security and management of these prisoners must also be in line with the following:
- [The Identification, Initial Categorisation and Management of Potential and Provisional Category A/Restricted Status Prisoners](#)
 - [The Review of Security Category - Category A/Restricted Status Prisoners](#)
 - [Management and Security of Category A Prisoners – Internal \(Restricted\)](#)
 - [Management and Security of Category A Prisoners - External Movements \(Restricted\)](#)
 - [Management of Restricted Status Prisoners \(to be published\)](#).

4.11 Referral of Offences to the Police

- 4.11.1 All suspected incidents of conveyance and/or possession of prohibited items must be investigated to establish whether there is a case for further action to be taken and the nature of that action. Serious offences must always be referred to the police for consideration for prosecution.
- 4.11.2 The [Crime in Prison Referral Agreement](#) provides guidance on cases which must be referred to the police for prosecution and Crown Prosecution Service (CPS) to pursue such prosecutions.
- 4.11.3 Prisons must take every opportunity to highlight to the police and CPS the damage caused to prisons and society by the presence of illicit items within their prison and press for a firmer line on referral for prosecution. See [Management and Handling of Evidence Policy Framework](#) for impact statements. Prisons have discretion to refer other conveyance item offences if there is a local agreement to do so or are other aggravating factors.

5. **Constraints**

Interdependencies

5.1 There are dependencies between this Policy Framework and the following policy documents:

- [Authorised Communications Controls and Interception Policy Framework](#)
- [Covert Testing Policy Framework \(to be published\)](#)
- [Counter corruption and Reporting Wrongdoing Policy Framework](#)
- [PSI 07/2015 PI 06/2015 Early Days in Custody](#)
- [Crime in Prison Referral Agreement](#)
- [Handling Mobile Phone Policy Framework \(to be published\)](#)
- [Health and safety arrangements: Management of Workplace Transport](#)
- [Health and Safety Arrangements for Radiation Safety of X Ray Security Equipment](#)
- [Health and Safety Arrangements for Risk Assessment PSI 37/2015](#)
- [Improvised Explosive Devices Policy Framework \(Restricted\)](#)
- [Incident Management Policy Framework \(Restricted\)](#)
- [Intelligence collection, management and dissemination in prisons and probation](#)
- [Management and Handling of Evidence Policy Framework](#)
- [Management of Internal Security Procedures Policy Framework \(Closed Prisons\)](#)
- [Management of security at visits Policy Framework \(Closed Prisons\)](#)
- [Management and Security of Category A Prisoners – Internal \(Restricted\)](#)
- [Management and Security of Category A Prisoners - External Movements \(Restricted\)](#)
- [Management of Restricted Status Prisoners \(to be published\)](#)
- [Managing prisoner safety in custody: Safety Policy Framework](#)
- [Managing the Local Security Strategy Policy Framework](#)
- [Pregnancy, MBUs and maternal separation in women's prisons Policy Framework](#)
- [Prison Adjudication Policy Framework](#)
- [PSI 49/2011 Prisoner communications policy](#)
- [Prison Dogs Policy Framework](#)
- [Public Protection Manual](#)
- [PSI 04/2018 Records Information Management Policy](#)
- [Searching Policy Framework](#)
- [PI 23/2014, PSI 27/2014 Security vetting: additional risk criteria for ex-offenders](#)
- [PSI 07/2014, PI 03/2014 Security vetting](#)
- [Serious and organised crime policy framework](#)
- [The Identification, Initial Categorisation and Management of Potential and Provisional Category A/Restricted Status Prisoners](#)
- [The Review of Security Category - Category A/Restricted Status Prisoners](#)
- [Use of CCTV \(Overt Closed-Circuit Television system\) Policy Framework](#)
- [Use of drug trace detection equipment in prisons Policy Framework](#)
- [Use of X-ray body scanners \(adult male prisons\) Policy Framework.](#)

Data Protection

5.2 Any information relating to an identified or identifiable living individual recorded as a consequence of this Framework will be processed in accordance with [The Data Protection Act 2018](#), [UK General Data Protection Regulation](#) and [Records Information Management Policy: PSI 04/2018](#). A full Data Protection Impact Assessment has been completed in support of this Policy Framework.

OFFICIAL

Freedom of Information Act 2000

- 5.3 This Policy Framework has been assessed as OFFICIAL and therefore suitable for public release. A number of supporting tools and linked policies have been marked as OFFICIAL-SENSITIVE and will not be available for public release.

Diversity and Inclusion

- 5.4 When communicating to staff, prisoners or visitors, Governors are expected to ensure that briefing documents and information is available in a variety of formats including easy read, braille, voice, and other languages.
- 5.5 Actions taken as a result of conveyance allow for an element of discretion and staff should be mindful of biases. These are the underlying attitudes and stereotypes that people unconsciously attribute to another person or group of people that affect how they understand and engage with them.
- 5.6 A full Equality Analysis has been completed in support of this Policy Framework.

Safety

- 5.7 An individual who is involved in conveyance of illicit items may themselves be vulnerable. Staff must be aware of this possibility and the support mechanisms in place for staff, prisoners, and visitors in these circumstances. See Support Links for Staff, Prisoners and Visitors (Annex X). It is important to be alert for any signs that a prisoner's risk of harm to themselves has increased and the consideration of ACCT monitoring. An individual who has had illicit items removed may also become violent to staff or other prisoners. More details of how to manage these situations are in [Managing prisoner safety in custody: Safety Policy Framework](#).
- 5.8 A prisoner who has been found in possession of illicit items as part of conveyance procedures set out within this Policy Framework may subsequently find themselves in debt. There are several measures that can be taken to mitigate the risk of prisoner debt created by the confiscation of property. This is of particular importance for those prisoners who are vulnerable, new, or recently returned to custody and/or during early days in custody. Governors can use the [HM Prison Service - Debt-Framework](#) to help manage debt.

Review

- 5.9 This Policy Framework and supporting impact assessments will be subject to ongoing review, responding to emerging changes and learning.

6. Guidance

The Guidance and supporting annexes work alongside the Policy Framework to assist closed prisons in managing the risk of conveyance and implementing the Requirements set out in Section 4.

6.1 Management of Conveyance General

Rehabilitative Culture

- 6.1.1 A rehabilitative culture is one where all the aspects of a prison culture support rehabilitation and contribute to a prison being safe, decent, hopeful, and supportive of change, progression and stopping offending. The application of security processes as outlined in

OFFICIAL

this Policy Framework should complement and underpin such a culture to ensure effective outcomes.

- 6.1.2 Traditional definitions of security are narrow and traditionally based on the prevention and detection of conveyance threats, and the management of the links with violence and ongoing criminality. This is a central aspect of prison security, but it is not all that security is or can be. People feel secure, not only when they are free from physical threat and violence, but also when they can exercise their rights, they expect to be treated fairly.
- 6.1.3 Procedural Justice (PJ) is one of the foundational features of a rehabilitative prison. Evidence shows that when people feel treated in procedurally just ways through Voice, Neutrality, Respect, and Trustworthy Motives, it contributes to a host of better outcomes, including well-being, rehabilitation/reduced recidivism, safety, and stability. Examples of how PJ can be considered in areas of conveyance and responding mitigations (i.e., visits, searching activities) can be accessed in the [Security-and-Rehabilitative-Culture-Sourcebook](#). Further information on PJ can be accessed via [Procedural justice](#).

Local Assessments

- 6.1.4 An evidence-based, prison wide, holistic approach should be used to identify, determine and justify mitigating measures to the threat and risk of conveyance in individual prisons. See Local Security Strategy Policy Framework for further information.
- 6.1.5 Governors and Directors may also choose to develop additional risk assessments to guide a local response to a potential risk that is unique to their prison.

Assurance

- 6.1.6 Assurance provides prisons with confidence that procedures are consistent and in accordance with policy. A good assurance process will provide confidence that security procedures are compliant with legislation and prisons LSS. See [Covert Testing Policy Framework \(to be published\)](#).

Notifications and Communications

- 6.1.7 Signage and information on the rights of access can be provided by the RiskandCapabilitiesUnit@justice.gov.uk. These can support prisons in managing the risk of content creators and auditors.

Reporting and Evidence Management

- 6.1.8 Any finds should be recorded on the IRS under the relevant heading or under the miscellaneous heading. A IR should also be submitted, as per the [Intelligence collection, management and dissemination in prisons and probation](#). All reports should include details of the illicit item/substance (if known) and location found. See [Incident Management Policy Framework \(Restricted\)](#) for further information.
- 6.1.9 An IR should be completed by the observing member of staff and should contain the minimum following information to assist in intelligence development:
- Location item found - Where were you when this happened? Where was the item secreted on the person or their belongings? Where do you think the person was intending on taking the item?
 - Grounds for suspicion - Why did you do what you did? How was the person behaving prior and afterwards? How were you alerted?

OFFICIAL

- Full description of the Item conveyed (if applicable) - How was it concealed? What packaging did it have? Any distinguishing features?
- Evidence bag number (if applicable).
- Person description (if applicable).
- IRS Number (if applicable).
- Actions taken.
- Any other information that is considered relevant.

6.1.10 Digital evidence such as mobile phones, SIM cards and items that have been used to access the internet should be considered for download via the Digital Media Investigation Unit (DMIU) by contacting dmiuforensics@justice.gov.uk.

6.1.11 Illicit items need to be secured as evidence in line with [Management and Handling of Evidence Policy Framework](#) which provides information on seizing evidence, exhibiting evidence, Health & Safety considerations.

6.1.12 The [Searching Policy Framework](#) provides guidance on positive indications provided by a technical aid. As a minimum the orderly officer should be contacted for further guidance in these circumstances. An IR should also be considered for an unexplained indication by a technical aid.

Support

6.1.13 There are several policies and processes that can help support staff, prisoners and visitors and should be considered when taking measures to reduce risk should an individual become vulnerable to conveyance. See Support Links for Staff, Prisoners and Visitors (Annex X).

6.2 Criminal Liability and Authorisations

When Crown Immunity for Crown Servants is available

6.2.1 Directly employed staff and other public servants (i.e., servants or agents of the Crown) can normally claim Crown immunity for offences under Section 40B, 40C, 40CA and 40D of the Prison Act if they contravene the provisions of the Act whilst carrying out their normal, designated work-related duties. If conveying or use of specific items clearly falls within the scope of a staff member's job, then there need not be any further action for Governors to take in setting out authorisations for these cases.

6.2.2 The availability of Crown immunity in respect of conveyance, use, and/or possession of prohibited items can avoid a multitude of local and central Prison Act authorisations which would otherwise be necessary.

6.2.3 Crown immunity is likely to apply to the circumstances where staff take out prisoner files to work on outside the prison where this is necessary for the fulfilment of their duties. This removes the need for a written authorisation under the terms of the Prison Act 1952 whenever a member of staff needs to take out a prisoner file. Staff whose normal duties involve taking out these files will be covered; those whose duties do not involve this activity will be committing an offence if they take out a file without permission.

Under an extension of Crown Immunity which is provided for by the Act for non-Crown Servants

6.2.4 Staff working in a prison who are not Crown Servants can have Crown immunity extended to them. Section 40F of the Prison Act allows for the Secretary of State to designate any

OFFICIAL

persons who work at a prison, but who are not Crown servants or agents, to be treated as if they were Crown servants. Once designated, they can claim on Crown immunity but only for purposes of the offences specified in section 40B to D of the Prison Act and if the conduct falls within the scope of their duties.

- 6.2.5 Crown immunity provides protection from prosecution for Crown servants who may commit a criminal offence as a consequence of carrying out their normal lawful duties.
- 6.2.6 The following persons are designated by the Secretary of State under section 40F of the Prison Act and as such shall be treated for the purposes of the application of sections 40B to 40D of the Prison Act as if they were doing that work as a servant or agent of the Crown:
- All staff working in contracted out prisons who are employed by the contractor operating the prison or contracted to that contractor for the provision of services within the prison on a regular basis.
 - All healthcare staff who are working in prisons and who are not crown servants.
 - All contract staff working in public sector prisons as part of a contract which is providing services within that prison on a regular basis.
 - All voluntary staff working in public or contracted out prisons who are providing services in that prison on a regular basis.
- 6.2.7 In addition to the above, workers contracted to HM Inspectorate of Prisons have been so designated as Crown servants for the purposes of the offences specified in section 40B to 40D of the Prison Act by the Secretary of State.

Authorisations for conveyance of items– Central and Local

- 6.2.8 The Prison Act prohibits certain items, referred to as List A, B and C items from being taken into or out of prisons, but there will be instances in which there are legitimate reasons why staff or professional visitors may seek to do things which would otherwise amount to an offence, for example:
- Take documentation or transmit information out of a prison.
 - Use cameras or sound-recording equipment within a prison.
 - Possess a device capable of transmitting or receiving images, sounds or information by electronic communications in a prison.
 - In accordance with [Faith and pastoral care for prisoners: PSI 05/2016](#).
 - Convey an offensive weapon for religious purposes (kirpan for example).
- 6.2.9 Items within List A, B and C include:
- List A – controlled drugs, explosives, firearms, ammunition, any other offensive weapon.
 - List B – alcohol, mobile phones, cameras, sound recording devices, articles designed or adapted for use with mobile telephones, cameras or sound recording devices (including disks, memory cards and wearable technology).
 - List C – tobacco, lighters and matchers, electronic cigarettes and vapes, money, clothing, food & drink, letters, papers, books, tools, Information Technology (IT) equipment (including component parts).
- 6.2.10 Items listed as A and B items require authorisation from the Secretary of State, PGD and/or Governing Governor when they are conveyed into and out of a prison.
- 6.2.11 The bringing in of items listed as C is only a problem and will only need authorisation if the intention is to give one of these items to a prisoner. This excludes IT equipment where an authorisation is required.

Central authorisations

- 6.2.12 Central authorisations are national authorisations that are automatically in place and do not require local approval. Guidance Table on Central/Local Authorisations (Annex F) provides examples of when a central authorisation is required or when an item can be approved locally.
- 6.2.13 All wearable technology requires a central authorisation under Section 40D and 40E of the Prison Act. They are classed as List B item and due to their functionality, smart watches are prohibited in prison unless prior authorisation is granted. A central authorisation will only be considered in exceptional medical circumstances where supporting medical documentation is supplied.
- 6.2.14 Although not a requirement, Governors may still request the submission of a local authorisation form for any items that have central authorisations in place. This could be to ensure prisons maintain local oversight of the items being conveyed.

Local authorisations

- 6.2.15 Prisons can issue local authorisations in certain circumstances, although individual written authorisations are not needed in the situations described in Guidance 6.2 Criminal Liability.
- 6.2.16 Local authorisations are normally issued to individuals and approved at a local level and may include the completion of a risk assessment to approve conveyance of the item. Local authorisations considered by Governors or by agreement from the PGD can be documented on a local form (see Template Form – Local Authorisation of Items Annex B) with the process set out in the LSS.
- 6.2.17 Examples of when local authorisations would be appropriate in relation to List A, B or C items could be:
- IT equipment and/or USB for the purpose of delivering training.
 - Cameras for use during assurance visits – audit, PGD etc.
 - Cameras for use during organised family visit days and/or celebrations (e.g., marriage)
 - Sound recording devices for use by Prison and Probation Ombudsman (PPO).
 - Conveying food into the prison for prisoners for example during a religious celebration.
 - Conveyance and possession of a kirpan (see Guidance on Authorisation for the Kirpan Annex G)

Local restrictions/Local lists

- 6.2.18 Local restrictions are local lists that include all list A, B and C items set out in sections 40A to 40F of the Prison Act but in addition, each Governor may publish additional restrictions and prohibit by local rules, the bringing in of a wider range of items and/or limit the amount of a specific list C item that can be brought in.
- 6.2.19 Local restrictions must still be adhered to although non-compliance will not be a criminal offence. Local lists should be reviewed regularly as part of the security meeting with any removal or addition of items documented changes should be in line with intelligence. Examples of local lists might be:
- Restricting the amount of certain list C items (e.g., money, drink or food) conveyed in to ensure searching measures are quick and effective, particularly in those prisons operating EGS.

OFFICIAL

- Introduction of paper-free policy for staff entering the prison in response to the threat of paper based Psychoactive Substance (PS).
- A central S40B authorisation has been provided for staff to bring in controlled drugs as part of prescribed medication subject to the member of staff seeking agreement from the Governor/Director or their nominated representative to do so. Local rules may prohibit the amount of medication brought in, for example only the amount required for the day.
- Restricting the number of bags individuals can bring in daily or implement a clear bag policy.
- Restricting aerosols, tobacco, vape liquid, chewing gum and other items that could pose a security risk.
- Requiring a solicitor to declare in advance they are bringing in IT equipment i.e., sound recording device. If the solicitor does not comply, then administrative action may be taken against the solicitor (assuming they were advised of the local regulation), but this doesn't also mean that the solicitor has committed a criminal offence as there is a central authorisation in place to make this action lawful in these circumstances. This includes memory sticks/USB which are component parts of IT.

6.2.20 It is important to ensure that local list restrictions are defensible and based on a local risk assessment led by intelligence. Local lists should be reviewed frequently responding to intelligence around risk. Blanket bans on items where there is no evidence of a local security risk and/or breach should not be considered. This is particularly important where the ban could indirectly affect groups of individuals on equality or other grounds.

6.3 Guidance of Managing Conveyance via the Gate

Vehicles entering

- 6.3.1 Vehicles arriving for delivery should park and report outside of the gate; the delivery arrival slot and process will vary by prison. Vehicles should be prioritised and processed as quickly as possible.
- 6.3.2 Managing Vehicle Gate Procedures (Annex I) includes key responsibilities of the gate staff, helpful tips, and minimum requirements. It can be used for staff who are new to the vehicle gate, or as a reminder for more experienced staff.
- 6.3.3 Guidance for Managers on Managing Deliveries (Annex K) includes key responsibilities, helpful tips, and minimum requirements that all managers who oversee vehicle gate processes must ensure the vehicle gate follows.
- 6.3.4 See [Security Risk & Capability Learning Hub](#) for more information and resources on conveyance via deliveries.

Vehicle searching and supervision

- 6.3.5 Searching equipment should always be well maintained and replaced as required. How this is done and by whom should be set out in the LSS. A system of managerial checks should also be in place to provide assurance of compliance in all these areas.
- 6.3.6 Dogs can also be used to assist in the searching of a vehicle or its contents. See [Prison Dogs Policy Framework](#).
- 6.3.7 Communication of the searching process and prohibited items should be in verbal, written, and pictorial form wherever possible. This will ensure that all people entering the prison are fully aware of the requirements. Individuals who are learning disabled or where English may not be their first language may find it more difficult to understand written communication.

OFFICIAL

- 6.3.8 Once the vehicle has entered the gate, staff should move the driver and any passengers away from the vehicle and conduct the level of search outlined in the Local Security Strategy. See [Searching Policy Framework](#).
- 6.3.9 Prior to this search, the driver and any passengers should be reminded of the unauthorised items list and advised that any items not disclosed will lead to a warning being issued.
- 6.3.10 Any items not covered by a central authorisation are to be surrendered to staff and held at the gate until the driver and any passengers leave the gate. Drivers and any passengers should be given access to secure lockers to store any possessions.
- 6.3.11 At this point, the delivery vehicle will be searched as per the procedures outlined in the LSS. The items in the vehicle will not usually be searched however the security department should direct when the delivery should be searched, on an intelligence led basis.
- 6.3.12 If an illicit item is located during the search of the person or vehicle and there is no immediate evidence that the conveyance or possession of the prohibited item is deliberate (for example an old lighter located under the driver's seat), then the prison should consider alternatives to issuing a warning or referring to the police (item dependent).
- 6.3.13 Actions will vary depending on the item, the circumstances of the case and the person involved. A deliberate attempt for example a box of lighters found under the driver's seat and concealed by clothing is much more serious and likely a deliberate attempt at conveyance.
- 6.3.14 On discovery of any item and provided the driver has previously been advised on entry of the articles not permitted into a prison, an informal warning should be given as a minimum and an IR submitted by staff.
- 6.3.15 Search staff should seek guidance from a manager on every occasion an illicit item is discovered.

Vehicle movement

- 6.3.16 All staff working in the gate and escorting vehicles should:
- Have received up-to-date security awareness training/briefing.
 - Control and monitor those whom they are escorting from the point of entry to the point of exit.
 - Know the identities of those they are escorting.
 - Possess a thorough knowledge of the geography of the prison and the areas in the prison to which those they are escorting are permitted access.
 - Be aware of local contingency plans.
 - Be proficient in the use of the prison radio net and any technical aids or equipment associated with the escorting role.
 - Be aware of the security and safety requirements of the prison and of the vehicle to be escorted.
 - Move vehicles to and from required destinations in a timely manner to meet the published local regime and requirements of other services.
- 6.3.17 Where vehicles are not escorted in accordance with the requirements of this Policy Framework, prior authorisation of these vehicles to enter should be requested from the communications/control room.

Emergency vehicles

6.3.18 In an emergency, it may not always be appropriate to search emergency vehicles on entry to a prison as the preservation of life takes precedence over local procedures. Emergency vehicles include Ambulance Service, Fire and Rescue Service, and Police Service. In an incident, this may also include Operational Response and Resilient Unit (ORRU) staff vehicles & responding tornado staff. In life threatening situations emergency vehicles will be allowed to leave without the need of a search of the vehicle to take place unless instructed otherwise by the manager.

6.3.19 Procedures that would normally apply to vehicles entering a prison may be suspended for responding ambulances. In most cases emergency vehicles will be given immediate access into the prison (see Quick Reference Guide - Emergency Vehicles Annex H). Other measures such as increased supervision and/or searching at the destination can be put in place to mitigate against any risks if considered appropriate.

Gate staff need to be aware there are central authorisations in place for when ambulances are required to enter the prison:

1. There is a central authorisation which approves for the conveyance into the prison of the onboard patient device which is a laptop/pad held in the ambulance containing the medical application (JRCALC). This device can be moved from the ambulance. There is no requirement to log this information at the gate especially in an emergency. Preservation of life takes precedent, where possible the device will be accounted for coming in and leaving the prison by a member of staff.
2. There is a central authorisation that permits entry of controlled drugs and supply of these to prisoners.
3. There is a central authorisation which permits ambulances to convey into and out of prisons, CCTV cameras that are fitted to their vehicles to record a potential incident.
4. A central authorisation is also in place for emergency services to enter with their mobile phones in situations where it is essential that a response is provided with minimal delay. These phones can be used by the staff to access the same medical apps as the onboard patient device and to contact the receiving hospital to enable quick and effective treatment. The following should be noted.
 - Only authorised ambulance staff are allowed to enter with phones.
 - Where possible phones should be accounted both on entering and leaving the prison.
 - Supervision of the staff should be in line with local processes.

6.3.20 Ambulance personnel will be required to secure all phones and personal devices not for clinical use in the emergency vehicle and should be switched off. Airwave radios and pagers can be retained on person.

Staff Vetting

6.3.23 Vetting is crucial in the protection against staff corruption. All Directly Employed (DE) and non-Directly Employed (NDE) staff must go through vetting. The Governor maintains ultimate authority in relation to decisions made concerning professional and official visitors only, their level of access to the prison and if normal security vetting checks are merited in cases where visits to the prison are frequent.

6.3.24 Information notices for staff on conveyance and the related provisions of the Prison Act should be displayed in the main gate and in other staffing areas. See Template Notice – Criminal Acts of Conveyance (Annex C) and Template Notice – Consequences of Conveyance (Annex D).

OFFICIAL

- 6.3.25 Staff should also be regularly reminded of the items they are not allowed to bring into the prison and the consequences of breaching these rules. This should be done as part of any induction process, as well as an annual reminder as part of the staff performance process.
- 6.3.26 There are several measures that can mitigate the risk of staff conveyance via the gate, examples of which may include:
- Robust staff searching as per the [Searching Policy Framework](#).
 - Before anyone is searched, advising them of those items that are prohibited inside a prison and any locally agreed lists. Staff should be invited to check themselves and any baggage for these items.
 - Providing staff, wherever it is practical to do so, with lockers or other means in which to store prohibited items such as mobile phones within the gate area prior to entry.
 - Considering mandating a bag used by prison staff to carry their belongings into the prison; this should be recorded in the LSS.
 - Processing staff mail in one area alongside all other mail. Where possible Governors can consider the use of the trace detection equipment and dogs to search this mail.
 - Reminding staff regularly of the requirements to disclose vulnerabilities and not just in the induction period.
 - Raising awareness through security communications of key concerns and support around corruption. Notices to staff, an effective induction process, corruption awareness training and initial officer training can all be used effectively to mitigate risk.
 - Raising staff awareness of the importance of managing media presence given digital capability is increasing within prisons and prisoners can access the internet illicitly and view social media which may provide vulnerable personal details.
 - Pro-social modelling by all staff, including managers, where employees act as a good motivating role model in order to bring out the best in people.
 - Developing a learning culture where mistakes are used as learning and staff are supported when they come forward about being pressured to convey items.
 - Effectively managing known and suspected corruptors (prisoners) within prisons to consider activity locations, residential accommodation, and monitoring.
 - Regular activity reviews for areas where prisoners (especially OCGs) may work closely with staff, e.g., red band positions and unit orderlies.
- 6.3.27 If a staff member is found with a controlled item i.e., vape liquids or chewing gum, there should be clear guidance on the process to be followed. This could include any or all of the following:
- Retaining the item for collection at the end of the day.
 - Issuing a verbal warning.
 - Issuing a written letter of guidance.
 - Documenting the find on a staff search log (to identify repeat offenders).
 - Initiating a managerial inquiry.
- 6.3.28 Governors are to refer to the [Crime in Prison Referral Agreement](#) for guidance on which offences to refer for a criminal investigation.
- 6.3.29 All finds should be reported on the intelligence system via a Corruption Prevention Intelligence Report (CPIR) to inform regional counter corruption teams.
- 6.3.30 The [Counter Corruption and Reporting Wrongdoing Policy Framework](#) outlines further information and actions.

OFFICIAL

6.3.31 See Staff Guidance on Reporting Corruption (Annex L) on actions for staff to take if they are asked by a prisoner to bring in illicit items.

Enhanced Gate Security

6.3.32 The following are identified key roles within Enhanced Gate Security (EGS).

- Head of Function: Governor/Director responsible for the gate complex.
- Security/Operations Manager (usually Custodial Manager): responsible for line management of Operational Support Grades (OSGs), supervising the maintenance of searching standards and quality assurance capability of equipment, monitoring EGS specific training and allocating staff to appropriate courses, ensuring that searching equipment is at optimum performance and acting as a local SPOC and link to Directorate of Security. This post will usually be assigned to Security/Operations and the individual selected will be assigned the responsibilities under this guidance.
- OSGs: staff working in the gate area responsible for carrying out searching. OSGs who are trained in operating the X-ray baggage scanner will be those carrying out and recording the daily safety check. OSGs should also undertake daily visual checks of the archway metal detector to ensure it is not damaged. Weekly checks by the operator should assess whether the unit is working at optimum performance. Additionally best practice for the baggage scanner includes:
 - Staff are advised to look through all images of the x-ray before coming to a decision if the bag is allowed to enter or further exploration is required.
 - Staff should spend a minimum of three minutes per bag when observing the images and coming to a decision.
 - Staff are to rotate every 20mins when operating the X-ray Baggage Scanner to ensure maximum effectiveness.
 - Use of a separate tray for key chains, work belts etc.
- Band 3 Officers: resource that can be deployed as required to support the gate searching process, areas of displacement, respond to incidents where powers of constable are required and enhance visible deterrence.
- Dog handlers: resource that is managed regionally and will support the gate searching process.
- Radiation Protection Adviser (RPA): nationally contracted third party responsible for providing advice on radiation protection and undertaking annual inspections and surveys of the X-ray baggage scanner equipment and reviews of radiation safety.
- Radiation Protection Supervisor (RPS): responsible for ensuring that the radiation operation is controlled in accordance with local rules and compliant with legislative requirements identified by the RPA, see Enhanced Gate Security - Baggage Scanner Local Rules (Annex E4). The RPS must have sufficient line management authority and time to undertake relevant duties as detailed in PSI 18/2015 - NOMS Health and Safety Arrangements for Radiation Safety of X Ray Security Equipment. There should be always an RPS on duty when EGS is operating, which will mean that prisons should have more than one trained RPS and should consider displaying who is the RPS on duty each day. See Enhanced Gate Security - Radiation Protection Supervisor Appointment Letter (Annex E3).

OFFICIAL

Items Entering the X-ray Baggage Scanner

6.3.33 Items that can and cannot enter the X-ray baggage scanner are outlined in X-ray Baggage Scanner and Items Entering (Annex E5).

Radiation safety

6.3.34 [PSI 18/2015 Health and Safety Arrangements for Radiation Safety of X Ray Security Equipment](#) advises that in relation to X-ray baggage scanner, it is not necessary to place restrictions on employees who are, or may become, pregnant though any concerns they raise should be addressed considerably. There is also no need to put any safeguards in place for pregnant visitors who will inevitably come into proximity to this equipment at the gate.

6.3.35 Electromagnetic field (EMF) testing is carried out by the manufacturer(s) of the archway metal detector and hand-held metal detector wands, which is part of their obtaining the Conformity European (CE) marking for their products. Following this, there are no EMF testing requirements for the equipment as the archway metal detectors and hand-held metal detector wands use low intensity EMFs/non-ionising radiation like mobile phone transmission.

Installation/Re-location of equipment

6.3.36 All prisons should contact RiskandCapabilitiesUnit@justice.gov.uk if they are considering moving the archway to an alternative location.

6.3.37 See [PSI 18/2015 Health and Safety Arrangements for Radiation Safety of X Ray Security Equipment](#) for policy requirement on the installation and re-location of equipment before its use.

Maintenance/Serviceing

6.3.38 For further information following installation, prisons should contact mojprocurementsecurity@justice.gov.uk and EGSPSMqueries@justice.gov.uk. Private prisons should ensure that a contract for maintaining this equipment is in place with a suitable supplier.

6.3.39 Service and maintenance records should be made available for audit purposes during the lifetime of the equipment.

External maintenance

6.3.40 Refer to Enhanced Gate Security - Summary Equipment Checks (Annex E2).

6.3.41 Each archway metal detector is programmed during installation. The archway settings should not be changed. As per the supplier installation and programming manual for the archway metal detector, a mandatory verification/re-certification of the calibration of the archway metal detector should be conducted every 12 months, and a record of this must be held. This task should be performed through the annual PPM plan or by prison staff if they have the right test kit. Contact RiskandCapabilitiesUnit@justice.gov.uk should you wish to change the settings.

6.3.42 The supplier will complete scheduled maintenance checks on the X-ray baggage scanner as per the agreement.

OFFICIAL

Prison owned assessments

6.3.43 The Head of Function may wish to involve the prisons Health and Safety Advisor(s) and contact RiskandCapabilitiesUnit@justice.gov.uk for X-ray baggage scanner specialist advice and support when conducting an ionising radiation risk assessment on the X-ray baggage scanner. See Ionising Radiation Assessment (Annex E1).

Procurement

6.3.44 HMPPS prisons source X-ray baggage scanners and archway metal detectors from MoJ commercial contracted suppliers, prisons can order new equipment via SOP and contact RiskandCapabilitiesUnit@justice.gov.uk or mojprocurementsecurity@justice.gov.uk for further advice.

6.3.45 Contracted Prisons are responsible for the purchasing and funding of their own X-ray baggage scanners and archway metal detectors in the absence of an agreed arrangement. However, it is strongly recommended that they look at the specifications of equipment used in public sector prisons to ensure that they source effective equipment which complies with legislative requirements and HMPPS' requirements for practice. Contracted prisons are still required to comply with HMPPS policies and instructions.

Training

6.3.46 OSGs should attend and complete the OSG training package provided by Learning and Development which incorporates EGS as an additional week. A record who has undertaken the training is to be held by the prison.

Audit arrangements

6.3.47 For both public sector prisons and contracted prisons the quality assurance audit will be undertaken by HMPPS Performance, Assurance & Risk Group (PAR) as part of the prison's security audit, and this will involve an audit of the physical searching process.

6.3.48 HMPPS health and safety function in liaison with the RPS and contracted RPA will undertake an annual assurance and monitoring for all public sector prisons, using the national health and safety audit and reporting tool. This audit will be used to monitor compliance with the [Ionising Radiation Regulations 2017](#) for the X-ray baggage scanner equipment.

6.3.49 The health and safety processes may be different for contracted prisons and therefore, contracted prisons must have their own health and safety arrangements which ensure, so far as is reasonably practicable, the health, safety and welfare of all employees, and others who may be affected using all EGS equipment.

Data collection

6.3.50 Prisons are asked to provide data about the use of EGS and are asked to provide this information in a timely manner to Risk and Capabilities Unit.

6.4 Guidance on Managing Conveyance via Reception

6.4.1 When assessing the security measures to tackle conveyance, consideration of the layout, staffing and size of the reception area will be required. Technical aids (hardware detection pole) will also need to be considered to address and identify routes of conveyance.

Reception searching

- 6.4.2 Where reception has been identified as an area of conveyance, as a minimum, Governors should:
- Where permitted by the [Searching Policy Framework](#) and the LSS, the prisoner may be full searched if not already routinely done so, using technical aids where available.
 - Where permitted by the [Searching Policy Framework](#) and the LSS, the prisoners in possession property may be fully searched using technical aids.
 - Update NOMIS including completing an IRS and submit an IR for any item found to ensure intelligence is communicated to future escorting staff and any future prisons.
 - Consider prisoner location; this is particularly important in cases where bullying/coercion is a suspected factor in prisoner conveyance.
 - Consider adjudication procedures as per Prison Adjudication Policy Framework.
- 6.4.3 Searching processes will be agreed locally based on an assessment of risk and detailed in the LSS. The types of searches that may apply are:
- Sterile area search - the sterile areas is a secure area in which to decant prisoners before entering reception. When staff are confident that the area does not contain any illicit items, the area is sterile. Where searching of the sterile area is required, it should be conducted before prisoners arrive and using a systematic method. For more information see [Searching Policy Framework](#).
 - Holding area search - a full search of holding and waiting areas in reception should be conducted where required to ensure that these areas are sterile upon reception of prisoners. For more information see [Searching Policy Framework](#).
 - Searching of person and property - refer to [Searching Policy Framework](#) for specific guidance, technical aids and instructions on searching prisoners and property in reception in all circumstances and prisons.
- 6.4.4 A multi-layered security approach in addition to searching can be successful in mitigating the risk of conveyance of illicit items. This includes:
- X-ray scanning to detect object and high volume of substances.
 - Search of the person.
 - Property cards check to verify if a property has been logged and belongs to a prisoner.
 - Use of drug trace equipment.
 - Contact with sending prisons to verify if a parcel originated from them.
 - Checking parcel's tracking number to establish if it came from another prison or a person.
 - Using official courier services and appropriate labelling to mark a parcel as a legitimate.
- 6.4.5 Prisons can use the services of thebigword to ensure that all information in relation to conveyance, searching and use of technical aids is communicated to those who don't speak English. Local diversity and inclusion leads can support prisons to make them accessible to people who are neurodiverse and with protected characteristics.
- 6.4.6 Receptions in prisons may wish to operate an amnesty process for illicit and unauthorised items for all prisoners arriving in reception. see Reception Amnesty Process (Annex P).

Prisoner property and parcels

- 6.4.7 Governors should ensure that staff working in reception are fully informed of the local facilities list in respect of prisoner's property and procedures are in place to ensure any updates to this are communicated appropriately.

OFFICIAL

- 6.4.8 [Prisoners' Property Policy Framework](#) sets out situations when Governors may temporarily or permanently confiscate any item found in the possession of a prisoner not authorised to have it. Any items confiscated by the Governor must be handed back upon the prisoner's permanent release.
- 6.4.9 Illicit items found within prisoner property can be varied, see Quick Reference Guide - Illicit Finds via Reception (Annex M). Prisoners may have concealed illicit items and substances in their property in possession and stored property. Concealment can be in radios, clothing, and canteen items. There have also been incidents of prisoners taking legitimate devices, such as PlayStation or Xbox consoles, and modifying them to enhance the device capability, such as the ability to access the internet. See Guidance on Games Consoles (Annex N).
- 6.4.10 Illicit items and substances normally drugs, SIM cards and tobacco can be concealed in items handed in on a visit. All property handed in on a visit should go via reception to ensure correct searching processes are applied.
- 6.4.11 Ad-hoc parcels sent in by associates may contain illicit items, however false excess property parcels are a more common way of illicit items entering the prison. This occurs when a prisoner is transferred to another prison and excess property is left behind. Associates may then use this method as a way of sending in a false parcel alleged to be the excess property sent on from the previous prison. False parcels are often constructed in a similar way to legitimate parcels to prevent detection.
- 6.4.12 Where it has been identified through intelligence that false excess property parcels are being used to convey illicit items, Governors are to ensure that all excess property packages purported to have been sent on by another prison are searched fully, even in respect of stored property. Refer to [Searching Policy Framework](#) for the process of searching property parcels, supporting tools and False Property Parcels (Annex O) for further information.
- 6.4.13 Prisons can utilise the use of drug trace equipment within reception areas for suspected presence of illicit substances and the drug seizures contract. See [Use of drug trace detection equipment in prisons Policy Framework](#).
- 6.4.14 In addition, prisoners returning from external escorts has also been identified as a route of conveyance when packages are picked up at the hospital. It is important to be vigilant around emergency A&E escorts and prisoners appearing to be keen to access a specific area within the hospital. This behaviour should be reported back to the prison so appropriate searching procedures can be implemented on return.

Prisoners at risk of conveyance and/or found to be conveying

- 6.4.15 The LSS should include local processes on managing prisoners at risk of conveyance and/or found to be conveying illicit items into the prison, this may include the use of dry cells in some prisons.
- 6.4.16 During discharge or reception of a prisoner as part of a police production, any security concerns in relation to conveyance should be immediately highlighted to the Duty Governor and any actions taken should consider the requirements outlined in [External Escorts Policy Framework](#).

Assessing a prisoner's risk of conveyance

OFFICIAL

- 6.4.17 By assessing a prisoner's risk of conveyance on reception, it can help to identify associates and organised criminality prisoners involved in other means of conveyance e.g., via visits.
- 6.4.18 Any prisoner may be at risk of conveying illicit items via reception however prisoners on ROTL may be more vulnerable or those with previous history to include:
- Prosecuted for conveying items.
 - Known to, but not prosecuted for conveying items.
 - Suspected of conveying items.
 - Known to be vulnerable to the conveyance of items.
- 6.4.19 Be aware that risks and ways of checking the risks may be different for a prisoner on initial (including repeat) reception, and prisoners being transferred from another prison.
- 6.4.20 The following can be checked to identify if a transferred prisoner may pose a risk of conveyance.
- Person Escort Record (PER) – the PER has a section specifically relating to known risk of phone/drug conveyance and the concealment of weapons/other items. It will also highlight when a prisoner is a risk to themselves or others.
 - Digital Prison Service (DPS) – this can be checked for adjudications relating to conveyance and can be done before the prisoner arrives.
 - Communication – the prisoner may be known to colleagues at the receiving prison, the transferring prison, or by escort staff as posing this risk.
 - Security and intelligence - the Security Department may have intelligence that the prisoner is concealing illicit items on transfer. Checks should be made, where possible, before the prisoner enters the prison to avoid distribution of illicit items. The Offender Management Unit (OMU) department should circulate details of transfers to several areas within the prison to include Safer Custody, Security and Healthcare. Where possible, checks should be made 24 hours before the prisoner arrives to provide an up-to-date picture of the risk. If it is not possible to check in advance of arrival these checks should be made while the prisoner is in reception.

Measures to take if a prisoner poses a risk of conveyance

- 6.4.21 The following actions should be taken:
- Any intelligence updated onto the PER, prisoner's NOMIS and an IR submitted. This ensures that the incident is communicated to all escort staff and any future prisons.
 - The prisoner may be offered amnesty upon entering reception if the prison operates this process.
 - Staff should interview prisoners who may be under threat to convey illicit items into the prison to ensure the appropriate support is put in place.
 - The prisoner should be full searched if not already routinely done so, using technical aids where applicable.
 - The prisoner's property should be fully searched and held back if required for this process (the prisoner can be offered 48hrs of initial kit). Searching of the property should be detailed, see the [Searching Policy Framework](#) for further guidance.
 - Additional staff should be allocated to reception to assist in the property search.
 - Staff should be made aware of the County Lines model and reporting. Organised criminals are exploiting vulnerable individuals to convey items into prisons.

6.5 Guidance on Managing Conveyance via Correspondence

Risk	Examples
Drug Supply	Drugs soaked on paper and secreted within paperwork

OFFICIAL

Violence and intimidation	Correspondence, bank details, telephone numbers that may not be on approved list
Escape	Maps of the prison, personal identification documents
Terrorist risk	Books, articles, letters, posters, artwork
Sexual/ Child Sexual Abuse & Exploitation offences	Explicit Pornographic material

Correspondence searching

6.5.1 Searching of correspondence is essential in the prevention of the conveyance of illicit items into a prison. Measures can include:

- Visual search to look for markings to the paper, addition of blank pages or suspicions about the sender.
- Physical search to feel for concealed items or thicker paper (sometimes PS-soaked paper is concealed within 2 other pieces to prevent detection by the trace detection equipment).
- Monitor the situation (attempt to identify associated intelligence gaps for targeted intervention).
- Trace detection equipment used for all mail as a deterrent.
- All mail subject to a dog search as a deterrent.
- Targeted mail monitoring (risk of increased bullying of the vulnerable to receive mail).
- Photocopying social prisoner mail.
- Use of trace detection equipment on all legal mail and percentage triangulation with legal companies in line with the [Use of drug trace detection equipment in prisons Policy Framework](#).
- Implementing a register/log for recoding incoming staff mail.
- Pin phone monitoring.
- X-ray machine to identify items hidden inside (SIM cards for example).

6.5.2 Policy requirement specifically around the interception of legal correspondence which can only take place when authorised by the Governor according to specific criteria can be found in the [Authorised Communications Controls and Interception Policy Framework](#).

6.5.3 The authority to photocopy mail can be found in [Authorised Communications Controls and Interception Policy Framework](#).

6.5.4 Prisons are to refer to [Public Protection Manual](#) for those prisoners that are subjected to restrictions and for information on banned material that applies to all prisoners.

Visually suspicious correspondence (legal and confidential)

6.5.5 Some legal and confidential mail may appear visually suspicious, therefore prior to testing the correspondence the mail staff should, in addition to the above:

- Check postal marks/franking stamps to see if these are old and inconsistent with the receipt of the letter.
- Maintain a correspondence log for suspicious legal mail so that patterns can be identified and investigated, ensuring that information is passed to security via an IR. Where there is reason to believe that the letter has not originated from a genuine

OFFICIAL

source, the prison should check directly with the firm or body, or individual concerned. Check with the security department for information about the prisoner if they are named on the envelope.

- Ensure post room staff have up to date intelligence about known current threats in the prison regarding legal and confidential mail, intelligence gaps to fill and are passing any information that may be useful.

6.5.6 See Guidance on Suspicious Correspondence & False R39 (Annex Q).

6.5.7 Prisons should consider the use of a unique reference number (URN) to support legal companies and the prison on addressing the current threat. For further guidance email hmppsdrugstrategy@justice.gov.uk. Those prisons that adopt this approach must consider that some legal companies may not be local and as such would not have the URN, therefore legal and confidential mail should still be processed as per [PSI 49/2011 Prisoner Communications Services](#).

Suspicious correspondence in prisoner possession

6.5.8 There will be occasions when prisoner correspondence enters the prison and is observed during an accommodation fabric and decency check, cell search or in reception and thought to be suspicious. There are several actions to take should this occur. The [Searching Policy Framework](#) provides some guidance on searching of paperwork to include correspondence. Key indicators that correspondence may be soaked in an illicit substance for distribution are.

- It is concealed within something else for example inside a stereo or pen.
- It is wrapped inside something else.
- It is torn into smaller sized pieces or similar sized sections have been removed.
- It is hidden somewhere on the person or secreted internally.
- It is being used to smoke or vape.
- It has been hidden within the fabric of the cell.

6.5.9 If it is suspected a prisoner is conveying items via correspondence, the prison should report suspicions to security via an IR, inform the orderly officer and request a cell search to be carried out and consider the use of search dogs, use of trace detection equipment and use of seizures contract. See Quick Reference Guide - Searching of Cells for Illicit Correspondence (Annex R).

6.6 Guidance on Managing Conveyance via the Perimeter

6.6.1 See Mitigating Conveyance via the Internal & External Perimeter (Annex S) and Control Measures against Conveyance via Perimeter (Annex T) for examples of actions that can be taken to mitigate the risk of conveyance via the perimeter.

Control/Communications rooms

6.6.2 In order to maintain correct radio discipline:

- Approved operating procedures for the network should be maintained.
- Areas of limited/nil reception should be identified and managed.
- Spare handsets should be securely stored.
- Only equipment from approved suppliers is used and the storage, issue, use, return and maintenance of radio network handsets is managed.

6.6.3 Staff working in the communications room should complete as a minimum: [CRFE: Control Room for Future Operatives eLearning \(mydevelopment.org.uk\)](#) and the face-to-face Prison

OFFICIAL

Radio Control Room Procedure course. The eLearning is a pre-requisite for the face-to-face course.

- 6.6.4 In order to effectively protect the prison from the risks posed by conveyance, all radio equipment should be designated as essential security equipment and be regularly and professionally maintained.

Incident management

- 6.6.5 Governors should consider set terminology for radio use to alert all staff to a possible throw overs or drone breach without alerting prisoners.
- 6.6.6 All persons to include staff, contractors, visitors, and prisoners should be made aware of the systems in place to raise the alarm in the event of throw overs or drone incident.
- 6.6.7 Communications and control room staff should be trained in the appropriate use of the radio net during these incidents. Local instructions may provide further details including guidance of seeking a response from specified outstations, e.g., Victor, Oscar and Sierra, dependant on type of incident. They should also provide the process for summoning external emergency assistance.

Internal movement

- 6.6.8 It is important to recognise that other types of prisoner movements take place within prisons that cannot be facilitated by main movement or individual ad hoc movement. These movements might include group or individual movement to activities such as healthcare clinics, evening education, physical education activities, or visits to reception for discharge.
- 6.6.9 Control/communications room staff will need to be able to manage the following.
- Control and authorise both routine and unscheduled movement of prisoners, staff, contractors, visitors, and vehicles within the prison.
 - Receive, evaluate, report and act upon information and indications of events.
 - Manage initial responses to events and emergencies.
 - Control and maintain the radio net and ensure secure usage.
 - Maintain secure practices and efficient operating procedures.
- 6.6.10 All internal movement of prisoners should be risk assessed locally and the relevant level of control and supervision provided to maintain security, control, order, and safety.
- 6.6.11 Areas that have been identified as “hot spots” for the collection and movement of illicit items should have additional measures in place to manage the risk, for example additional staffing or more controlled movement. This may include specific work areas that are located close to the external perimeter and vulnerable to throw overs/drone activity or activities where illicit items are passed to others in the prison.
- 6.6.12 Where security concerns dictate that additional security measures are required to restrict the conveyance of illicit items in a specific scenario (for example movement to religious services) a risk assessment should be completed to consider and address the implications of any searching measures before the movement takes place. This should include.
- Any emerging intelligence.
 - Previous intelligence and history of conveyance via this process.
 - Type of prisoners involved in this movement and any equality implications.
 - Numbers of prisoners likely to be searched.

OFFICIAL

- Measures taken to reduce impact of additional searching measures (additional time for ablutions for example in the case of searching prior to religious services).

6.6.13 All staff involved in internal prisoner movements will need to be competent in the use of a prison radio and understand the procedure to alert the control/communication room to an identified throw over or other breach of the perimeter as part of the movement process.

6.6.14 In relation to the risk of escape and internal movement see the [Management of Internal Security Procedures Policy Framework \(Closed Prisons\)](#).

Exercise yards and activity areas

6.6.15 Governors should assess the risk and likelihood of illicit items being thrown into exercise yards and external activity areas via the perimeter. This should take account of the following:

- Current or previous intelligence.
- Proximity of the area to the perimeter.
- Security procedures in place – CCTV, covered yards etc.
- Type of prisoners able to access the area.
- Level of staff supervision in the area.
- Bushes, foliage, and other things that could enable items to be hidden.

Drone activity

6.6.16 Drones are a growing threat which are used to convey illicit items into prison and can be a significant security risk. Drones are used by criminals, including those involved in Serious and Organised Crime (SOC), to deliver contraband into prisons. Drones can carry large payloads of contraband which can cause sudden deteriorations in the safety and security of prisons. New legislation came into effect on the 25th January 2024 making it an offence to pilot a drone within the vicinity of Prisons and Young Offender Institutions without an exemption. Guidance can be found at - [Drone Restricted Airspace around Prisons & Young Offender Institutions in England and Wales - GOV.UK \(www.gov.uk\)](#).

6.6.17 It is an offence under 40D of the Prison Act 1952 for a person who, without authorisation takes a photograph, or makes a sound-recording, inside a prison, this includes images taken by drones.

6.7 Guidance on Managing Conveyance via Visits

6.7.1 The consequences of conveyance and the criminal offence that may be committed by the conveyance of illicit items into the prisons should be communicated via notices placed in the visitor's centre and searching areas for both prisoners and visitors. All prisons should clearly display up-to-date information on local policies and procedures, specifically regarding restricted items (List, A, B and C Annex A). See the [Management of security at visits Policy Framework \(Closed Prisons\)](#) for further information.

Approved conveyance

6.7.2 A central authorisations is in place for the approved conveyance and use of IT and other equipment by official visitors. See Guidance on IT Equipment Authorisation for Official Visitors (Annex U). Only if there is sound intelligence that this facility is being misused (i.e., one that could be defended in court), should restrictions be put in place.

Tackling conveyance of illicit items

- 6.7.3 There are several ways visitors may convey items to prisoners during visits. Staff can refer to the [Management of security at visits Policy Framework \(Closed Prisons\)](#) for further guidance.
- 6.7.4 There is a promising practice learning guide on managing visits and preventing conveyance which can be accessed here [Security Risk & Capability Learning Hub - Domestic Visits Promising Practice Learning Guide](#).
- 6.7.5 Staff should be fully aware of the risks associated with conveyance via visits and the measures required to tackle this. Quick Reference Guide - Managing a Pass on Visits (Annex V) provides a quick reference guide on how to manage a pass on visits and Tackling Conveyance via Visits (Annex W) provides information on best practice, risk areas and how to identify conveyance.
- 6.7.6 To prevent conveyance, staff working in visits should:
- Place an amnesty box outside the prison creating a clear 'point of no return'.
 - Search all visitors before entering the visits area. See the [Searching Policy Framework](#) for searching instructions and use of technical aids.
 - Search prisoners upon leaving the visits area. Prisons LSS should set out the requirements for frequency of searching following visits.
 - Search visits areas before and after visits take place.
 - Check the bins for the disposal of items that may later be brought into the prison
 - Ensure that shared toilet facilities are not used by prisoners and visitors at the same time and that following the use of shared facilities, those facilities are searched before the visit is allowed to continue.
 - Ensure that where refreshments are purchased during visits, they are served without packaging, for example on plates or in transparent cups.
 - Ensure that prisoners and visitors are not swapping clothing or footwear and that prisoners are wearing the same clothing when leaving the visits area.
 - Ensure that staff can always supervise all visitors and prisoners with correct positioning of staff, furniture, use of CCTV and Body Worn Video Cameras (BWVC).
 - Adopt a digital approach to official visits only allowing the entry of laptop computers by official visitors with a view to stopping paper. This would minimise the threat from PS and there is a central authorisation in place for laptop computers.
 - Consider a contactless payment option in the visit's canteen. restricting the use of cash.
 - Submit IRs where there has been suspected/proven conveyance of such items.
 - Ensure that policies and procedures are communicated to staff and followed in respect of any internal secretion of illicit items to include swallowing. This will include medical attention where appropriate.
- 6.7.7 A controlled visits area will assist prisons in reducing passes of illicit items during the visit session. Each prison will have a different process for the allocation of staff working in visits. Where conveyance via visits is a significant threat, Governors should consider the use of a dedicated visits group where this is achievable.
- 6.7.8 The member of staff in charge of visits should also brief staff working in visits on any potential threats or persons of interest, before visits commence. Staff can then ensure that any persons of interest are seated appropriately and in clear view of CCTV.
- 6.7.9 The implementation of an acceptable standard of dress by visitors is also a good deterrent to passing of items. Some clothing items can all allow for a quicker and more discreet

OFFICIAL

method of removing illicit items ready to pass. A notice should be clearly displayed advising prisoners and visitors of any local policy information regarding acceptable behaviour and physical contact in the visit areas. This should include the consequences of non-compliance. Staff should be fully briefed on this.

6.7.10 Governors should ensure that all staff are clear on the agreed process for breaching any local policy during a visit. This can be any of the following but is not limited to this list alone:

- Prolonged or excessive physical contact.
- Moving of furniture to obscure view.
- Contact with children where a prisoner is restricted from doing so.
- Passing of prohibited items.
- Swapping clothing.
- Drinking from an unlidged cup.
- Drinking from the same cup as your visitor (sharing cups).
- Use of abusive/foul language or behaviour to staff, visitors, or prisoners.
- Aggressive/ violent behaviour.
- Refusal to comply with searching and other local policy and procedures.
- Any behaviour which facilitates or engages in criminal activity.
- Prisoners having visits with other prisoner's visitors during the visit session, unless agreed in advance by the Governor.

6.7.11 An awareness of equality issues during the visit process specifically regarding religious clothing and individuals who are learning disabled is fundamental to ensuring an inclusive process. See [Searching Policy Framework](#).

Assurance

6.7.12 Preventing conveyance via visits is most effective when staff are trained in searching procedures and carrying out their duties in line with the LSS. It is mandated for staff to undertake training in X-ray baggage scanner operation before its use. There should be management oversight and monitoring in place to ensure the process is compliant.

7. Annexes

7.1 Official Sensitive annexes can be accessed here [National Security Framework \(NSF\)](#).

Annex A	List A, B & C Items
Annex B	OFFICIAL-SENSITIVE - Template Form - Local Authorisation of Items
Annex C	Template Notice - Criminal Acts of Conveyance
Annex D	Template Notice - Consequences of Conveyance
Annex E1	Ionising Radiation Assessment
Annex E2	Enhanced Gate Security - Summary of Equipment Check
Annex E3	Enhanced Gate Security - Radiation Protection Supervisor Appointment Letter
Annex E4	Enhanced Gate Security - Baggage Scanner Local Rules
Annex E5	OFFICIAL-SENSITIVE - X-ray Baggage Scanner and Items Entering
Annex F	OFFICIAL-SENSITIVE - Guidance Table on Central/Local Authorisations
Annex G	OFFICIAL-SENSITIVE - Guidance on Authorisation for the kirpan
Annex H	OFFICIAL-SENSITIVE - Quick Reference Guide – Emergency Vehicles
Annex I	OFFICIAL-SENSITIVE - Managing Vehicle Gate Procedures

OFFICIAL

Annex J	OFFICIAL-SENSITIVE - Guidance on Workshop Deliveries
Annex K	OFFICIAL-SENSITIVE - Guidance for Managers on Managing Deliveries
Annex L	OFFICIAL-SENSITIVE - Staff Guidance on Reporting Corruption
Annex M	OFFICIAL-SENSITIVE - Quick Reference Guide - Illicit Finds via Reception
Annex N	OFFICIAL-SENSITIVE - Guidance on Games Consoles
Annex O	OFFICIAL-SENSITIVE - False Property Parcels
Annex P	OFFICIAL-SENSITIVE - Reception Amnesty Process
Annex Q	OFFICIAL-SENSITIVE - Guidance on Suspicious Correspondence & False R39
Annex R	OFFICIAL-SENSITIVE - Quick Reference Guide – Searching of Cells for Illicit Correspondence
Annex S	OFFICIAL-SENSITIVE - Mitigating Conveyance via the Internal & External Perimeter
Annex T	OFFICIAL-SENSITIVE - Control Measures against Conveyance via Perimeter
Annex U	OFFICIAL-SENSITIVE - Guidance on IT Equipment Authorisation for Official Visitors
Annex V	OFFICIAL-SENSITIVE - Quick Reference Guide – Managing a Pass on Visits
Annex W	OFFICIAL-SENSITIVE - Tackling Conveyance via Visits
Annex X	OFFICIAL-SENSITIVE - Support Links for Staff, Prisoners and Visitors