HM Prison & Probation Service

Ministry of Justice

Policy name: Authorised Communications Controls and Interception Policy Framework

Reference: N/A

Re-issue Date: 09 June 2025

Implementation Date:

- **From 20 September 2022 -** All sections, excluding section 23 (Enhanced Contact Vetting).
- **From June 2025 -** Section 23.1 – 23.54.

Replaces the following documents (e.g. PSIs. PSOs, Custodial Service Specs, Policy Frameworks) which are hereby cancelled:

- PSI 04/2016 - The Interception of Communications in Prisons and Security Measures.

Introduces amendments to the following documents:

- Managing Extremism and Terrorism Amongst Offenders in Custody: Policy Framework.
- Managing Extremism and Terrorism Amongst Offenders in Custody: Detailed Guidance.
- PSI 43/2014 - Management and Security of Category A Prisoners.
- PSI 09/2015 - The Identification, Initial Categorisation and Management of Potential and Provisional Category A / Restricted Status Prisoners.
- PSI 49/2011 – Prisoner Communication Servicess.
- PSI 18/2016 – Public Protection Manual.
- Management of Security at Visits (Open Estate).
- Management of Security at Visits (Closed Estate).
- Secure Social Video Calling Interim Policy Framework.
- Use of Drug Trace Detection Equipment in prisons Policy Framework
- 2022 Separation Centres Operating Manual.

Action required by:

☒	HMPPS HQ	☒	Governors
☒	Public Sector Prisons	☒	Heads of Group
☒	Contracted Prisons	☒	The Probation Service
☒	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: The aim of this Policy Framework is to produce clearer and more enhanced risk-based guidance for prisons on managing and mitigating the risks associated with authorised communications, across all prisons in England and Wales.

By the implementation date governors of public sector prisons and contracted prisons and heads of probation delivery units must ensure that any new local policies that they develop because of this Policy Framework are compliant with relevant legislation, including the public-sector equality duty (Equality Act, 2010).

This Policy Framework is supported by the accompanying Authorised Communications Controls Detailed Guidance and the Interception and Restriction of Communications Operations Manual designed to support delivery of the mandatory requirements set out in this Policy Framework. Whilst this guidance will not all be mandatory, any deviation from what is set out in this guidance must be documented locally. Any questions concerning deviation from the guidance can be sent to the contact details below.

Any such local procedures must be suitably analysed, or risk assessed to meet the requirements of the public sector equality duty, the Data Protection Act 2018, the family test and required financial and other resources.

'Governor' includes an officer for the time being in charge of a prison. Any reference to 'governor' in this Policy Framework includes any director of a contract managed prison. Any reference to 'Prison Group Director' (PGD) means the Deputy Director of contracted custodial services when referring to any contract managed establishment. Any reference to governor also includes the delegated functional head.

The term 'prisoner', for the purposes of this Policy Framework, applies to adults, children and young people.

How will this Policy Framework be audited or monitored?

Mandatory elements of this Policy Framework should be subject to local management checks and may be subject to self or peer audit by operational line management/HQ managers, when deemed appropriate by the managers with responsibility for delivery. Local management checks should be documented in establishments' Local Security Strategy. For further guidance on local management checks, please see section 22 in relation to interception, of the Interception and Restriction of Communications Operations Manual.

Mandatory elements of this Policy Framework will be subject to quality assurance checks by HMPPS Operational and Systems Assurance Group (OSAG) through the Security Audit.

In public prisons and Young Offender Institutions (YOIs) PGDs will monitor compliance with requirements set out within the Policy Framework in their prisons.

In contracted prisons and YOIs monitoring of compliance will be through the standard contract management processes.

The Investigatory Powers Commissioners Office (IPCO) provides oversight of interception and restriction arrangements in prisons and conducts inspections of prisons, ensuring these powers are used in accordance with the law.

Resource Impact: This Authorised Communications Controls and Interception Policy Framework replaces *Prison Service Instruction (PSI) 04/2016 The Interception of Communications in Prisons and Security Measures*. It also provides updates relevant to a number of policies related to authorised communications controls. Therefore, many of the mandatory requirements are not new. There are new requirements that have an impact on resources, specifically in relation to the Enhanced Contact Vetting (ECV) scheme for terrorist prisoners and prisoners on remand for terrorism offences. This will be absorbed mostly by the Joint Extremism Unit, with the support of CT Policing. There will be some impact on the resource of establishments, including initial local resource implications as establishments update Local

Security Strategies and align with new procedures. A detailed resource impact assessment accompanies this Policy Framework.

Contact

For enquiries about interception, restrictions and PIN phone management, please contact: Intelligence.ProjectsPolicy@justice.gov.uk.

For enquiries about Enhanced Contact Vetting please contact: ECV@justice.gov.uk

Deputy/Group Director sign-off: Richard Vince, Executive Director of Directorate of Security.

Approved by OPS for publication: Sarah Coccia and Ian Barrow, Joint Chairs, Operational Policy Sub-board, 28th May 2025.

Revisions

27 September 2022	Update to the contact email for the Approved Contact Scheme
15 February 2023	Update regarding the Approved Contact Scheme – which will be implemented in 2023 (exact date to be confirmed)
16 March 2023	Update to contact details on Page 3
5 April 2023	Revised Annex B
7 June 2023	Revised Annex B
27 October 2023	Revised Annex B
23 November 2023	Revised Annex B
05 January 2024	A number of amendments to ensure policy coverage of new communication platforms, to support improving operational compliance and resilience with regard to interception and PIN phone management and to more effectively align communication restrictions and monitoring with the relevant policies – specifically PSI 49/2011, PSI 18/2016 and PSI 43/2014.
06 November 2024	Revised Annex B
14 February 2025	Paragraphs 21.1 and 21.2 amended
8 April 2025	Revised Annex B
09 June 2025	Paragraph 23 updated to reflect new Enhanced Contact Vetting process. Redefined ‘terrorist prisoner’ in paragraph 3.13 to align with broader HMPPS policy. Deleted deficient sentence at the end of paragraph 9.8.

CONTENTS

Section	Title	Page
1.	**Purpose**	5-6
2.	**Outcomes**	6-7
3.	**Requirements**	8-48
4.	**Annexes**	49
Annex A	Notification for Prisoner and Contact Subject to Communication Restriction	
Annex B	Confidential Access List - List of Confidential Access Organisations	
Annex C	Communications Compact -To be signed by the prisoner upon reception. The simple version is to be used as an aide.	
Annex D	Intercepted Privileged Telecommunications and Mail Log - To be completed when any legal/confidential telecommunications are recorded and/or monitored in error or deliberate circumstances	
Annex E	Formal Notification of Live Monitoring -- A paper copy is to be given to the prisoner before live monitoring commences	

1. Purpose

1.1 Prison Rule 4 / YOI Rule 42(2) stipulates that special attention shall be paid to the maintenance of such relationships between a prisoner and their family, as are desirable in the best interests of both, and that prisoners shall be encouraged and assisted to establish and maintain such relations with persons and agencies outside prison as may, in the opinion of the governor, best promote the interests of his[1] family and his own social rehabilitation.

1.2 This is integral to a prisoner's right to family life as their rehabilitation and visits are crucial to sustaining relationships with close relatives, partners, and friends, where appropriate, and help maintain links within the community. However, certain restrictions are necessary to protect the public, prevent crime and ensure the security of the prison.

1.3 HMPPS meets this requirement by allowing prisoners to communicate and maintain ties with family and friends, and to communicate with legal advisers and other professionals. HMPPS also ensures that legal advisers and some other organisations with whom they may correspond is done so in a way that ensures legal privilege and/or confidentiality. Prisoners can communicate in the form of written communications (including email), telephone calls, video calls and (where present) in-cell messages (further referred to as telecommunications) and visits.

1.4 Whilst HMPPS recognises the importance of allowing prisoners to communicate, authorised methods of communications can be exploited for illicit purposes and there may be circumstances where it is necessary and proportionate to place restrictions or conditions on communications. The purpose of this framework is to provide guidance and mandatory actions that will govern communications controls and interception available to governors.

1.5 This policy sets out the Enhanced Contact Vetting (ECV) scheme, which requires the vetting of contacts for all convicted terrorist prisoners and prisoners on remand for terrorism offences and, if judged to be necessary and proportionate, **[REDACTED]**. To support the delivery of the ECV scheme, a dedicated ECV team has been established.

1.6 This Policy Framework applies necessary and proportionate controls under the ECV scheme to vet contacts and, where appropriate, restrict communications through visits, telephone calls, video calling and in writing (including email) to mitigate potential security threats and protect the public.

1.7 This Policy Framework will also provide clear guidance to decision makers in respect of the legal basis upon which controls can be put in place, to ensure compliance with the following:

- The Investigatory Powers Act 2016.
- Prison Rule 34 - permits the restriction of communications.
- Prison Rule 35A to 35D – permits the interception of communications
- Prison Rule 35 – relating to personal letters and visits.
- Prison Rule 38 – outlining the grounds of legal visits.
- Prison Rule 39 - regarding the delivery and receipt of legally privileged material.
- Prison Rule 73 - permits governors to prohibit visits by a person to a prison or prisoner, in certain circumstances.

[1] Please note that this paragraph quotes directly from the relevant legislation, and references to gender reflect the original text. In terms of the scope of this policy, the content should be considered applicable to all demographics.

- Prison Rule 81 - permits governors to devolve the powers and duties of interception to another officer of that prison.
- Young Offenders Institution (YOI) Rules (9 – 15): Parallels prison rules 34, 35, and 35 A-D), for young offenders.
- Human Rights Act 1998 and the European Convention on Human Rights.

1.8 Content within the Policy Framework regarding interception of communications will ensure the consistent application of powers available to HMPPS under the Investigatory Powers Act 2016 (IPA) and Prison Rule 35A – 35D/YOI Rules 9-15.

1.9 Content within the Policy Framework regarding the restriction of communications will ensure the consistent application of powers available to HMPPS under the Investigatory Powers Act 2016 (IPA) and Prison Rule 34/YOI Rules 9-15.

1.10 Detailed guidance and background information for operational staff working in any areas affected by instructions for interception and restriction of communications will be provided via an *Interception and Restriction of Communications Operations Manual* which has been restricted to protect HMPPS tactics from exposure. The National Intelligence Unit will circulate this to governors for controlled distribution to those undertaking the duties referenced within.

2. Outcomes

2.1 The desired outcomes of this Policy Framework are that:

a) All prisoners can communicate and maintain ties with family and friends and communicate confidentially with legal advisers and other professionals in a manner which does not compromise safety.

b) The process meets policy and legal requirements and ensures that the security and good order of the prison is maintained, and the public are protected.

c) HMPPS can, where necessary and proportionate in accordance with Prison Rule 35A/YOI Rule 11, **intercept** communications through telephone calls, video calls and written (including digital) methods for the following reasons:

- the interests of national security;
- the prevention, detection, investigation or prosecution of crime;
- the interests of public safety;
- securing or maintaining prison security or good order and discipline in prison;
- the protection of health or morals; or
- the protection of the rights and freedoms of any person.

d) HMPPS can, where necessary and proportionate and compatible with ECHR rights in accordance with Prison Rule 34/YOI Rule 9, **restrict** communications or impose conditions through telephone calls, video calls and written (including digital) methods for the following reasons:

- the interests of national security;
- the prevention, detection, investigation or prosecution of crime;
- the interests of public safety;
- securing or maintaining prison security or good order and discipline in prison;
- the protection of health or morals;
- the protection of the reputation of others;

- maintaining the authority and impartiality of the judiciary; or
- the protection of the rights and freedoms of any person.

In accordance with Prison Rule 34(4) HMPPS can also impose closed visits. Subject to paragraph (2) above, the Secretary of State may require that any visit, or class of visits, shall be held in facilities which include special features restricting or preventing physical contact between a prisoner and a visitor.

f) HMPPS can, where necessary and proportionate in accordance with Prison Rule 73/YOI Rule 9, **ban certain visitors** for the following reasons:

- the interests of national security;
- the prevention, detection, investigation or prosecution of crime;
- the interests of public safety;
- securing or maintaining prison security or good order and discipline in prison;
- the protection of health or morals;
- the protection of the reputation of others; or
- the protection of the rights and freedoms of any person.

However, Prison Rule 73 does not apply to visits by a member of the Independent Monitoring Board (IMB), Justice of the Peace or to prevent any visit by a legal adviser for the purposes of an interview under Prison Rule 38 or visit allowed by the IMB under Prison Rule 35(6).

g) All staff in HMPPS and the contracted estate understand what constitutes the correct management of PIN phone systems, prisoner contact lists, written correspondence, intercept activity, and their legal obligations.

h) HMPPS records all social telecommunications (this includes telephone calls, secure social video calls and in-cell messages) by default, it being necessary and proportionate to do so. Written social correspondence, including emails, can be intercepted and monitored when necessary and proportionate to the outcomes being sought by the prison.

i) HMPPS manages the processes associated with PIN phone systems and prisoner contacts in line with the relevant legislation and enables prisoners to maintain positive social contacts unless it is necessary and proportionate to impose a restriction.

j) Prisoners' ability to communicate with legal contacts and organisations given confidential access is facilitated subject to controls under Prison Rule 35A(2A), Prison Rule 38 (visits from legal advisers), Prison Rule 39 (delivery and receipt of legally privileged material) and YOI Rule 17.

k) Applications for the use of vetting controls, interception or restriction and visitor bans are submitted and vetted in accordance with provisions of this policy framework and accompanying guidance. The applications are subject to proper scrutiny and review and are managed robustly throughout the lifespan of vetting, interception, and restriction. Additionally, all actions and decisions are recorded, retained and disseminated in line with auditing requirements.

3. Requirements

Definitions

3.1 *A contact of concern* may include:

- An ex-prisoner who was either (i) at any time category A or (ii) is managed under **[REDACTED]**[2], except where the person is a close relative in accordance with paragraph 3.12.
- A serving prisoner with a former prisoner who was either (i) at any time category A or (ii) is currently managed under **[REDACTED]** except where the person is a close relative in accordance with paragraph 3.12.
- Content or individuals/organisations where there is intelligence or a reasonable suspicion that it/they (including the prisoner themselves) promote or support acts of terrorism (as defined by Terrorism Act 2000) and extremism[3] (further referred to as "terrorist concern" in this Policy Framework).
- An individual who is identified through intelligence or a reasonable suspicion as being at risk of coercion, harassment, domestic abuse, or harm by the prisoner, including intimidating a witness and/or threatening a victim.
- A person who has previously helped or planned to help the prisoner in an escape attempt or a person for whom there is intelligence or a reasonable suspicion that they are helping or planning to help the prisoner in an escape attempt.
- Where there is intelligence or a reasonable suspicion that contact would be placing a child's welfare at risk.
- A person for whom there is intelligence or a reasonable suspicion that they are committing crimes on the prisoner's or other prisoners' behalf.
- A person for whom there is intelligence or a reasonable suspicion that they are managing the proceeds of the prisoner's crimes.
- A person who is currently on bail or undergoing criminal investigation except where the person is a close relative in accordance with paragraph 3.12.
- A person subject to terrorism prevention and investigation measures or licence conditions which prohibit contact with the relevant prisoner.
- Correspondence between a prisoner who is under 18 and other person or organisation would not be in that prisoner's best interests except where the person is a close relative in accordance with paragraph 3.12.
- Planning to use the visits to collect material for publication (e.g. journalistic material, webpage material) or where the prisoner is seeking publicity for their crimes or circumstances at that time, in circumstances where this is not permitted by *PSI 37/2010* and there is no overriding public interest in allowing contact.

3.2 *Interception* is defined under Prison Rule 35A (6) / YOI Rule 11(6) as:

(a) In relation to a communication by means of a telecommunications system, means any action taken in relation to the system or its operation so as to make some or all of the contents of the communications available, while being transmitted, to a person other than the sender or intended recipient of the communication; and the contents of a communication are to be taken to be made available to a person while being transmitted where the contents of the communication, while being transmitted, are diverted or recorded so as to be available to a person subsequently; and

[2] **[REDACTED]**
[3] As defined by the UK government in March 2024 - New definition of extremism (2024) - GOV.UK

(b) in relation to any written or drawn communication, includes opening, reading, examining and copying the communication.

3.3 *Restriction* is defined in Prison Rule 34(8) (b) / YOI Rule 9 (8)(b) as including restrictions and conditions in relation to the length, duration and frequency of communications. Prison Rule 34 / YOI Rule 9 applies to all communications with a prisoner, including communications in visits.

3.4 *Particular Action* refers to restricting a specific instance of communication (telecommunication, written correspondence or visits) between a prisoner and a particular contact (address/individual), where it is necessary and proportionate.

3.5 *General Action* refers to restricting all communications between a prisoner and a particular contact (address/individual), enabling governors to take longer term action where the risks/issues between a prisoner and a particular contact are not mitigated through particular action and restricting all communications between the prisoner and a particular contact is necessary and proportionate.

3.6 *Intelligence Reports (IR)* are used to submit and evaluate information, and to manage the dissemination of intelligence. They protect the source and also contribute to an audit trail of the intelligence.

3.7 An *Official Video Call* is a form of communication using a telecommunication system, between prisoners and their legal advisors and/or other official bodies, as defined in Rule 2 of the Prison Rule 1999 and Young Offender Institution Rules 2000.

3.8 *Social Video Calls* were introduced to help maintain family contact for those held in custody whilst physical visits were impacted by the restrictions of COVID-19. The social video calls currently operate alongside, not as a replacement for, face-to-face social visits.

3.9 *In-cell Messaging* is a form of telecommunication that allows messages to be sent to/from a prisoner using an authorised app-based system. Such systems are linked to the PIN phone (or equivalent) telephone system.

3.10 *Social visits* are visits from friends, family members (including family days) or Official Prison Visitors (OPVs). OPVs are independent volunteers appointed by governors to visit and offer friendship to prisoners. For more information on OPVs and other types of visitors please see *PSI 16/2011 – Providing Visits and Services to Visitors.*

3.11 *An official visit* as defined by *PSI 16/2011 – Providing Visits and Services to Visitors.*, is a visit by the following persons. These visits do not require the prisoner to use a visiting order or count against his/her allowance of social visits:

a) Legal advisers
b) Offender managers/probation staff
c) Social workers/Youth Offending Team (YOT) workers
d) Pastoral visits by authorised and appointed faith leaders / representatives to visit those prisoners registered as belonging to their faith
e) Bishops
f) Samaritans
g) MPs, Welsh Assembly Members or MEPs visiting in an official constituency capacity
h) Officers of the Parliamentary and Health Service Ombudsman
i) Representatives of the Prison and Probation Ombudsman, the Legal Ombudsman, the Quality Care Commission, and the Office of the Legal Services Ombudsman

j) Authorised researchers
k) Embassy or consular officials
l) Police officers or other public officials in discharge of their duty
m) Visits from an accredited agent of the Treasury Solicitor, the Director of Public Prosecutions, the Crown Prosecution Service, or the Official Receiver in Bankruptcy, on production of the necessary authority from the department, to interview and to serve documents on a prisoner
n) Staff of the Criminal Cases Review Commission
o) Representatives of veterans organisations such as the Royal British Legion, the Soldiers Sailors Airmen and Families Association when acting in an official capacity or assisting with resettlement issues
p) Representatives of the Equality and Human Rights Commission (EHRC) visiting in a professional capacity or any other organisation when the purpose of the visit is specifically and solely to discuss equality issues
q) Immigration Officers or representatives of the United Kingdom Border Agency
r) Visits by other officials or bodies to whom confidential access arrangements applies

This is not a definitive list. If a prisoner requests an official visit from an organisation or individual not listed above, governors may decide the conditions in which it takes place. Official status may also be extended to interviews by officers of other investigative bodies such as HM Revenue & Customs, the Security Service, the Serious Fraud Office, the Crown Prosecution Service and equivalent bodies of other countries. Legal visits are subject to Prison Rule 38 (YOI Rule 16).

3.12 A *close relative* is defined in paragraph 2.23 of *PSI 49/2011 – Prisoner Communication Services* as follows:

- Spouse/partner (including a person -whether of the same or different sex - with whom the prisoner was living as a couple in an established relationship immediately prior to imprisonment)
- Parent
- Child
- Brother, Sister (including half, or step - brothers and sisters)
- Civil Partner
- Fiancé or Fiancée (provided that the governor is satisfied that a bona fide engagement to marry exists)
- A person who has been acting in loco parentis to a prisoner
- A person to whom the prisoner has been in loco parentis.
- Grandparents
- Those who have clearly demonstrated the intention to register a civil partnership but have not yet done so may also be included within this definition of close relative for the purposes of any form of communication.

This definition of “close relative” is distinct from the interpretation of a prisoner’s “immediate family” which appears in *Chapter 2 Section 2 of the PSI 18/2016 – Public Protection Manual.*

3.13 *A terrorist prisoner* refers to (a) someone convicted of a specified terrorism offence as set out in Part 1 or Part 2 of Schedule 19ZA of the Criminal Justice Act 2003, or (b) someone whose offence is deemed to have a terrorism connection, as defined in section 247A of the Criminal Justice Act 2003.

Overview

4.1 Governors must ensure that local arrangements are in place to vet, restrict or intercept social communications in accordance with Prison Rules 34/YOI Rule 9 (restrictions or conditions (e.g. vetting contacts)), 35A/YOI Rule 11 (interception), Prison Rules 73 YOI Rule 9 (visits), only where necessary and proportionate, and on the grounds set out in those Rules.

4.2 This policy provides guidelines regarding the vetting of contacts (known as the Enhanced Contact Vetting scheme) of terrorist prisoners, prisoners on remand for terrorism offences and, if judged to be necessary and proportionate, **[REDACTED]**. Governors must ensure that local arrangements are in place to implement the ECV scheme in accordance with section 23 of this Policy Framework.

4.3 Where the communications relate to **[REDACTED]**, Serious and Organised Crime (SOC)[4] or Crime and Corruption Unit (CCU)[5] nominals, the relevant regional lead must be consulted at the earliest opportunity – the decision on restrictions, conditions or monitoring however is the governors'.

4.4 Decisions to restrict, intercept communications or apply the ECV scheme, must be supported by evidence, or a reasonable assessment that such action is necessary and proportionate for its intended purposes and particular care needs to be taken to ensure that individuals are not targeted simply based on any protected characteristic.

4.5 *The Equality Act 2010* lists age; disability; gender reassignment; marriage and civil partnerships; pregnancy and maternity; race; religion or belief; sex and sexual orientation as protected characteristics, protected under the Act. Governors and their staff should, therefore, never discriminate against prisoners by applying the controls in this policy based on protected characteristics.

4.6 Governors may delegate their responsibility to officers to intercept, monitor, restrict or vet communications in accordance with Prison Rule 81/YOI Rule 85. Such delegation must be confirmed electronically using secure email/documentation and kept for audit purposes by the delegator. This delegation must be reaffirmed in an email when there is a change of governor, or in the case that a new member of staff is devolved the power. Further guidance regarding the roles and responsibilities of staff engaging in the interception of communications is contained in the *Interception and Restriction of Communications Operations Manual.*

4.7 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 *PSI 04/2018 - Records, Information Management and Retention Policy*. Prisoner personal information must be requested, obtained, used and held in accordance with: *HM Prisons Prisoner Privacy Notice.* Visitors personal information must be requested, obtained, used and held in accordance with the *HM Prisons Visitors Privacy Notice*. A full Data Protection Impact Assessment has been

[4] Refers to individuals planning, co-ordinating and committing serious offences, whether individually, in groups and/or as part of transnational networks. The main categories of serious offences covered are; child sexual exploitation and abuse, illegal drugs, illegal firearms, fraud, money laundering and other economic crime, bribery and corruption, organised immigration crime, modern slavery and human trafficking and cyber-crime.

[5] 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. In prison and probation services, this would include the misuse of a person's role to plan or commit a criminal act, or a deliberate failure to act to prevent criminal behaviour. For a non-exhaustive list of examples of criminal activities and / or inappropriate behaviours that fall within this definition of corruption, alongside further information regarding the CCU, please refer to Counter Corruption and Reporting Wrongdoing Policy Framework (publishing.service.gov.uk).

completed, to accompany this Policy Framework. Contact dataprotection@justice.gov.uk for further advice.

Contact of Concern

5.1 It is evident within prisons that direct abuse of authorised prison communications through visits, telephone calls, video calls and/or written communications does occur, and is a tactic utilised by some cohorts of prisoners. Whilst most communications into the community will be for legitimate reasons, it is evidenced that some prisoners communicate with other prisoners, family, friends, or members of the same criminal network for reasons including to organise reoffending; share victim details; threaten or control others and convey illicit items[6]. Friends and family are also used as a third party to communicate with prisoners in other prisons and victims, and to continue illicit activity[7].

5.2 Governors must ensure that arrangements are in place to identify potential contacts of concern, as set out within sections 3 and 4 in the *Authorised Communications Controls Detailed Guidance.*

5.3 When a governor identifies a contact of concern, the Communications Action Decision Process, in section 3 of the *Authorised Communications Controls Detailed Guidance*, can assist in determining what action(s) should be taken.

5.4 Having identified a contact of concern, governors must consider whether restrictions or conditions should be put in place and which restrictions, or conditions should be put in place. Contact must only be prevented to the extent to which it is necessary and proportionate.

5.5 Where a contact of concern (as described in paragraph 3.1), is identified, in order to restrict, intercept, or vet contacts (where relevant), it must be necessary and proportionate to do so in accordance with Prison Rules 34/YOI Rule 9 (restrictions or conditions (e.g. vetting contacts), 35A/YOI Rule 11 (interception), Prison Rules 73 YOI Rule 9 (visits) as relevant.

Communication Controls

5.6 There are **four** key communication mitigation options available to governors, having followed the Communications Action Decision Process, in section 3 in the *Authorised Communications Controls Detailed Guidance*:

1. **Restrictions** (of mail, email, telephone, social video calling and/or internet use), see paragraphs 6.1 to 6.18, and 9.10 to 9.11.
2. **Closed visits and banning visitors**, see paragraphs 7.1 to 7.8 and the *Management of Security at Visits (Open Estate and Management of Security at visits (Closed Estate) Policy Frameworks.*
3. **Interception and Monitoring where not already authorised,** see paragraphs 13.1 to 17.26 and the *Interception and Restriction of Communications Operations Manual*.
4. **Applying the Enhanced Contact Vetting (ECV) scheme,** see section 23.

5.7 Where imposing one form of communication mitigation, governors must consider whether additional communication restrictions (see section 6) monitoring (see section 13), visitor

[6] Illicit items mean property for which it is a criminal offence to have in possession and could lead to prosecution.
[7] Illicit activity means activity that is criminal and could lead to prosecution.

restrictions (see paras 7.1-7.8) or vetting (if not previously subject to the ECV scheme) are required. If the governor decides that:

a) communications restrictions are required, they must complete Annex 1 - Op Manual. Where the ECV scheme applies, the governor must consider reviewing contact permissions under the scheme.
b) communications monitoring is required, they must complete Annex 2 - Op Manual.
c) visitor restrictions are required, they must complete Annex 2 - Detailed Guidance. Where the ECV scheme applies, the governor must consider reviewing contact permissions under the scheme.
d) the ECV scheme should apply to a prisoner, they must complete Annex 8.

The Restriction[8] of Communications[9]

6.1 Under Prison Rule 34 / YOI Rule 9 the Secretary of State may impose any restriction or condition, either generally or in a particular case upon the communications to be permitted between a prisoner and other persons if considered that the restriction or condition to be enforced does not interfere with the ECHR rights of any person under the Human Rights Act 1998; or

a) is necessary on grounds specified in paragraph 6.2 below;
b) reliance on the grounds is compatible with the ECHR right to be interfered with; and
c) the restriction or condition is proportionate to what is sought to be achieved.

6.2 The grounds referred to above are:

a) the interests of national security;
b) the prevention, detection, investigation or prosecution of crime;
c) the interests of public safety;
d) securing or maintaining prison security or good order and discipline in prison;
e) the protection of health or morals;
f) the protection of the reputation of others;
g) maintaining the authority and impartiality of the judiciary; or
h) the protection of the rights and freedoms of any person.

6.3 In addition to the specific restriction requirements set out in this Policy Framework or other national policy, which are imposed on an estate-wide basis, the restriction of communications must be approved by an Authorising Officer (AO), a role that should be undertaken by the functional Head of Security, and/or the functional Head of Offender Management. As with the interception of communications, these powers are delegated to the AO by the governor (public prisons) or Director (privately managed prisons), who has responsibility for the restriction of communications. Any delegation must be confirmed in an email and stored by the delegator electronically for audit trail purposes. Their role will include managing the process of restricting communications in accordance with policy and the law. All AOs and deputies must have sufficient knowledge and training to undertake the role.

<u>Restrictions on Telecommunications and Written Communications</u>

[8] Restriction is defined in Rule 34(8) (b) as including restrictions and conditions concerning the length, duration and frequency of communications. Rule 34 applies to all communications with an offender, including communications in visits (Rule 34(8) (a)).
[9] The policy on the restriction of communications (paragraphs 6.1 – 6.20) is owned by the National Intelligence Unit.

6.4 Where it is appropriate to restrict communications in accordance with Prison Rule 34 / YOI Rule 9:

a) The Application for the Restriction of Communications form (Annex 1 "Application for the Authorisation of the Restriction of Communications" in the *Interception and Restriction of Communications Operations Manual*) must be completed and authorised before restrictions are applied, unless:
   I. during live monitoring in which paragraphs 9.2 - 9.9 apply.
   II. the restriction is being applied in line with PSI 18/2016 – Public Protection Manual (see paragraph 6.5).

b) Governors and AOs must ensure that grounds for restrictions are met before taking any action, and any refusals of applications to restrict are documented on the application. For applications relating to those under the age of 18, consideration must be given to the likely greater impact this intrusion will have and the proportionality should take into account the age of the person it is being applied to.

c) Governors and AOs must ensure that the prisoner and the contact is informed of the restriction using the letter in Annex A "Notification for Prisoner subject to Communication Restrictions" including broad reasons as to why (subject to the exceptions described in para 6.9).

d) Staff must electronically attach any applications and authorisations to restrict communications to the prisoner's profile on the prison intelligence system.

e) Staff, AOs and governors must ensure that the relevant sections of the form are completed each time a restriction is renewed, and that these are attached to the prisoner's profile on the prison intelligence system.

6.5 *PSI 18/2016 – Public Protection Manual* outlines policy and guidance relating to restrictions that are applied on public protection grounds. These include:

a) Restrictions applied in relation to victims (both known and subsequently identified).
b) Restrictions applied in relation to non-contact requests made by members of the public, including by a person or authority with primary responsibility for a child, and by third parties making the request with the consent of the subject.
c) Restrictions applied by court order or injunction preventing contact.
d) Prisoners identified as presenting a risk, or potential risk, to, children.
e) Unconvicted prisoners who are identified as posing a risk of witness intimidation.

In these cases, the process outlined in paragraph 6.4 and the Communications Action Decision Process in section 3 of the *Authorised Communications Controls Detailed Guidance* do not need to be followed; instead, the requirements outlined in PSI 18/2016 – Public Protection Manual should be.

6.6 Should it be identified that a non-contact request does not have the consent of the member of public in question, then staff must follow the process outlined in 6.4 to ensure that any restriction applied is necessary and proportionate. Any information supplied in the request may be considered when deciding whether a restriction is necessary and proportionate.

6.7 Prisoners subject to the ECV scheme must only be permitted to communicate with those who are on their ECV Contact List. See Section 23 of this Policy Framework for further guidance on the application of the ECV scheme. Prisoners who are subject to Approved Visitors Scheme (AVS) must only be permitted to communicate with those who are on their AVS Approved Contact List. See Section 4 of *PSI 43/2014 Management and Security of Category A Prisoners*. for further instruction on the application of AVS.

6.8 Communications between convicted prisoners requires the approval of the governors of both the prisons concerned. Where the prisoners are close relatives (as defined by para 3.12) or where they were co-defendants at their trial and the correspondence relates to their conviction or sentence, approval must be given unless it is necessary and proportionate on one of the following grounds to prevent the prisoners from communicating:

a) the interests of national security;
b) the prevention, detection, investigation or prosecution of crime;
c) the interests of public safety;
d) securing or maintaining prison security or good order and discipline in prison;
e) the protection of health or morals;
f) the protection of the reputation of others;
g) maintaining the authority and impartiality of the judiciary; or
h) the protection of the rights and freedoms of any person

and the risks identified cannot be adequately managed by monitoring or placing other controls on the correspondence. For all prisoners, checks must also be made to ensure that they are not already prohibited from contacting each other (where directed by the courts or one of them has made a non-contact request for example). Accordingly, if the governor of the sending establishment has no objections, the letter should be sent to the governor of the recipient's establishment with a covering note inviting them to consider whether it should be issued. Where approval is given, communications may be made subject to monitoring or other controls. Should either or both prisoners be subject to the ECV scheme or the AVS, they must only be permitted to contact each other or other prisoners if they are on their list of approved contacts. For further guidance on the process for inter-prison communications, *see section 7.4* of the *Interception and Restriction of Communications Operations Manual.*

6.9 Where restrictions are authorised, establishments must check whether the prisoner is subject to the ECV scheme or the Approved Visitors Scheme (AVS). All decisions taken in relation to the restriction of communications for a terrorist, terrorist remand **[REDACTED]**, must be reported to the National Counter-Terrorism Communication Controls Centre (NCTCCC) and a copy of Annex 1 "Application for the Authorisation of the Restriction of Communications" (in the *Interception and Restriction of Communications Operations* Manual) sent to **[REDACTED]**.

6.10 Where a restriction is imposed through the process outlined in para 6.4, sufficient reasons must be disclosed to the prisoner to explain why it is necessary and proportionate to restrict contact in accordance with Prison Rule 34/YOI Rule 9. Disclosure must be made using the letter template in Annex A "Notification for Prisoner subject to Communication Restrictions". However, information can be withheld from disclosure to the prisoner if necessary for one of the following reasons:

a) In the interests of national security;
b) For the prevention, detection, investigation or prosecution of crime or disorder,
c) For the maintenance of prison security and good order and discipline in prison;
d) For the protection of a third party who may be put at risk if the information is disclosed;
e) if, on medical or psychiatric grounds, it is felt necessary to withhold information where the mental and/or physical health of the prisoner or a third party could be impaired; where the source of the information is a victim, and disclosure without their consent would breach any duty of confidence owed to that victim or would generally prejudice the future supply of such information. Where disclosure is prohibited by law.

A security alert must be placed on to the prisoner's account on PNOMIS[10] / Digital Prison Service (DPS) with the start and end date of the restriction.

6.11 Communications can be restricted during a telecommunications call if it is identified during live monitoring to be necessary and proportionate to do so. The Restriction of Communications application form in Annex 1 "Application for the Authorisation of the Restriction of Communications" of the *Interception and Restriction of Communications Operations Manual* must be completed following any restriction applied, and before further calls to that contact take place. Further consideration must be made as to whether ongoing restrictions are required.

6.12 All restrictions applied for under the process outlined in 6.4 will expire three months from the date of approval but can be renewed if it is considered necessary and proportionate to extend the period of the restriction. Renewals must be authorised by the last day of the existing period of restriction and documented on the restriction of communications application form in Annex 1 "Application for the Authorisation of the Restriction of Communications" of the *Interception and Restriction of Communications Operations Manual* and retained electronically for audit purposes. For applications that have been made following information and intelligence sharing with partner agencies and forums, the renewal must include any relevant updates and input from these sources that supports a decision on either the necessity and proportionality of ongoing restrictions. Restrictions can be cancelled before the end of the three-month period, for example if there is a change in risk identified. The reasons for the cancellation must be documented in the relevant section of the application.

6.13 Where communication restrictions are to be applied to a particular number or address, but a close relative sharing those contact details requires the ability to communicate with the prisoner, staff must be mindful that the restriction should relate to the social contact it has been applied against. Staff must therefore identify a workable solution to ensure proportionate application of the restriction – for example, identification of another contact number that will be used by the close relative or consideration of additional communication controls to manage any risk.

Management of Restriction – Telecommunications and Written Communications

6.14 The restriction of communications of a specific prisoner should be applied by the establishment they are residing in, unless it is considered necessary and proportionate to block a number more widely across the estate (for example, at a global level). In these cases, a request to apply the restriction must be made to the Central Authorities Bureau (CAB)[11] and the request must include the completed Annex 1 "Application for the Authorisation of the Restriction of Communications" within the *Interception and Restriction of Communications Operations Manual*. The governor must ensure that the establishment's Local Security Strategy sets out the arrangements for the management of restrictions once approved. These arrangements must include consideration of whether partial restrictions are more proportionate than total bans and an approach to managing attempts to circumvent them - for example, barring of numbers locally to prevent other prisoners adding the number to their PIN account on behalf of the prisoner or the monitoring of any correspondence to an address to which contact restrictions apply.

[10]PNOMIS – Prisoner National Offender Management System.

[11]Central Authorities Bureau: The CAB authorise and assure the use of Investigatory Powers across HMPPS and support the operational front line in use of these powers to tackle criminal activity.

6.15 On reception, staff must consider relevant documentation (e.g., Prisoner Escort Record (PER) or police/CPS MG6 form) to determine whether any restrictions need to be applied to a prisoner's communications. The Local Security Strategy must ensure a process for informing the relevant departments (e.g., mail room) of any restrictions applied is implemented and followed. For specific guidance on category A prisoners subject to AVS, s*ection 4 of PSI 43/2014 Management and Security of Category A Prisoners*.

6.16 All completed Applications to Restrict Communications (Annex 1 "Application for the Authorisation of the Restriction of Communications" in the *Interception and Restriction of Communications Operations Manual*) must be retained locally for auditing purposes.

6.17 Further guidance on the restriction of communications is set out in the corresponding section of the *Interception and Restriction of Communications Operations Manual.*

6.18 Governors and AOs should ensure staff are aware that, in line with Prison Rule 34(8)/YOI Rule 9(8), the restriction of all communication between a prisoner and a specific contact will extend to communications during visits. The management of visitor bans should be undertaken in line with the Management of Security at Visits - Open Estate Policy Framework and the Management of Security at Visits - Closed Estate Policy Framework.

The Banning of Visitors

7.1 For all matters relating to the security, facilitation and management of visits, including applying closed visits, please see *Management of Security at Visits (Open Estate* and Closed Estate) and *PSI 16/2011 – Providing Visits and Services to Visitors.*

7.2 For policy and guidance on all visitor bans please see the *Management of Security at Visits (Open Estate and Closed Estate).*

7.3 In addition to the reasons set out in the *Management of Security at Visits (Open Estate* paragraphs 5.43 – 5.45 and Closed Estate paragraphs 5.64 – 5.66) and in accordance with the relevant grounds, visitors[12] may also be banned where there is intelligence or a reasonable suspicion that the visit is promoting or supporting acts of terrorism (as defined by the *Terrorism Act 2000*) or extremism[13]. This is further referred to as "terrorist concern".

.

7.4 There must be clear justification for a ban, irrespective of which grounds are used. Bans on the grounds of "terrorist concern" may only be imposed if the policy requirements set out in paragraphs 4.25 to 4.44 of the *Management of Security at Visits (Open Estate and Closed Estate)* are followed.

7.5 Where visit restrictions are being considered or subject to review where there is a "terrorist concern" (in accordance with paragraph 7.3), an Application for Banning Visitors (for terrorist-concern purposes only) at Annex 2 "Application for the Authorisation of Banning Visitors (for Terrorist Concern Purposes Only)" in the *Authorised Communications Controls Detailed Guidance* must be completed. When doing so governors must consult the NCTCCC, before taking any action, although the decision is for the governor. Any comments from NCTCCC must also be included in the application, which must be sent to the NCTCCC upon completion. Copies should also be retained locally electronically for audit purposes.

[12] Prison Rule 73 does not apply in relation to any visit to a prison or prisoner by a member of the independent monitoring board of the prison, or justice of the peace, or to prevent any visit by a legal adviser for the purposes of an interview under rule 38 or visit allowed by the independent monitoring board under rule 35(6).

[13] As defined by the UK Governments Counter Extremism Strategy 2015.

7.6 NCTCCC must ensure they notify a prisoner and contact if they are subject to a visit/visitor ban under the grounds set out in paragraph 7.3 only, using Annex M found within the *Management of Security at Visits Policy Framework (Closed Estate)* and/or Annex K within the Closed Estate.

7.7 Governors must ensure each ban is reviewed at least every month in accordance with the *Management of Security at Visits (Open Estate and Management of Security at Visits Policy Framework (Closed Estate).* Where the review relates to terrorist prisoners **[REDACTED]**, the NCTCCC must be consulted as part of the review.

7.8 Further guidance on banning visitors under the grounds set out in paragraph 7.3 is set out in section 5 in the *Authorised Communications Controls Detailed Guidance.*

The Interception of Communications

8.1 In addition to the requirements in this Policy Framework, governors, Directors and AOs have the power to authorise the interception of communications, in line with any restrictions and requirements outlined in this Policy Framework, to gather intelligence and information to assist in the detection and prevention of crime and other national interest and community safety issues, the reduction of harm to vulnerable persons and to identify developing threats in an establishment and region.

8.2 Each of the interception powers available to HMPPS is overseen by a Senior Responsible Owner (SRO), who are supported in this role by a function which provides the central retrievable record.

8.3 The SRO for powers under *Investigatory Powers Act 2016* is the Executive Director of the Directorate of Security, or other nominated senior civil servant.

8.4 Investigatory Powers Commissioner's Office (IPCO) provides oversight of interception arrangements in prisons and conducts inspections of prisons.[14]

Requirements for Staff

8.5 Other than where this Policy Framework requires interception to be carried out, the monitoring of intercepted communications should be authorised by an AO, a role that should be undertaken by the functional Head of Security, and/or the functional Head of Offender Management (for offence-related monitoring). In privately managed prisons, the Director has responsibility for the restriction and monitoring of communications and therefore may delegate powers to the functional Head of Security and Offender Management like public sector prisons. Within the National Intelligence Unit (NIU), the monitoring of prisoner communications retained on digital/cloud platforms should be authorised by staff of Band 8 or above. In all cases at least one deputy must be identified to cover periods of absence. Any delegation must be confirmed in an email and stored by the delegator electronically for audit trail purposes. Their role will include managing the process of restricting and intercepting communications in accordance with policy and the law. All AOs and deputies must have sufficient knowledge and training to undertake the role.

8.6 Governors, NIU Band 8s and AOs must ensure that those delivering the requirements outlined in this section are locally assessed as competent to undertake the duties related

[14] IPCO independently review applications from public authorities to use the most intrusive of these powers and check that all the powers are used in accordance with the law.

their role. Local training can be provided by experienced staff, through use of the *Interception and Restriction of Communications Operations Manual*, or from formal training provision where this is available.

8.7 Governors, NIU Band 8s, prison senior managers (particularly in Security departments and the OMU) and AOs for the restriction and interception of communication must read the whole instruction and ensure that the Local Security Strategy (LSS) and local procedures comply with this chapter.

8.8 All staff engaged in the activities within this chapter must be trained in the submission of intelligence reports (IRs) and have the resource and ability to conduct these tasks when required. Staff in reception and induction roles are required to understand the process for interception in order to provide prisoners with accurate information.

The Management of Prisoner Communications and Interception Activity

9.1 In certain circumstances described below, governors and senior managers[15] with appropriate delegated authority can authorise the interception of a prisoner's communications and/or restrict prisoners' communications. Communications by a prisoner with their legal adviser or a confidential access organisation are not intercepted unless the governor or senior manager, with appropriate delegated authority, reasonably believes that the communication is being made with the intention of furthering a criminal purpose and unless the requirements and processes outlined in 15.1 – 15.7 are followed.

Restrictions on Communications on Reception into Prison, Where Live Monitoring Applies and on Internet Use

9.2 Under Prison Rule 34(2) / YOI Rule 9(A) the Secretary of State may impose any restriction[16] or condition, either generally or in a particular case, upon the communications to be permitted between a prisoner and other persons if he considers that the restriction or condition to be enforced does not interfere with the ECHR rights of any person under the *Human Rights Act 1998*; or

a) is necessary on grounds specified in paragraph 9.3
b) reliance on the grounds is compatible with the convention right to be interfered with; and
c) the restriction or condition is proportionate to what is sought to be achieved.

9.3 The grounds referred to above are:

a) the interests of national security;
b) the prevention, detection, investigation or prosecution of crime;
c) the interests of public safety;
d) securing or maintaining prison security or good order and discipline in prison;
e) the protection of health or morals;
f) the protection of the reputation of others;
g) maintaining the authority and impartiality of the judiciary; or
h) the protection of the rights and freedoms of any person.

[15] Senior Management: A prison manager of Band 7 or above or NIU Band 8 or above. Within privately managed prisons, the equivalent will be at least D2 grade in G4S managed prisons, H2 grade in Sodexo managed prisons and Assistant Director grade in Serco managed prisons. F*or all other operators that may operate privately managed prisons in the future, this must be a competent member of staff as approved by the Director at functional head level.*

[16] Restriction is defined in Rule 34(8) (b) as including restrictions and conditions concerning the length, duration and frequency of communications. Rule 34 applies to all communications with a prisoner, including communications in visits (Rule 34(8) ()). Restrictions in relation to visits is covered in section 7 of this Policy Framework.

9.4 Further information on restricting prisoner communications outside of the management of the PIN phone system, and restrictions on the use of the internet, can be found in section 6 and section 9.

9.5 Upon initial reception into custody, prisoners who are subject to the ECV scheme or AVS will have additional layers of contact vetting and restrictions applied, and these will replace the processes relating to adding and approving social contacts outlined in paragraph 9.6. For AVS requirements, please refer to s*ection 4 of PSI 43/2014 Management and Security of Category A Prisoners*. All prisoners must sign the Communications Compact.

9.6 Prisoners must not make phone calls until their PIN phone account has been officially set up in line with *PSI 49/2011 – Prisoner Communication Services* and the relevant security checks and processes for adding contact numbers to the PIN phone system outlined within this Policy Framework have been followed. The process for the signing of the Communications Compact should be undertaken within 24 hours of reception, unless the prisoner is received during weekend hours in which the process should be undertaken within 24 hours of weekday operational hours commencing. The process of setting up the PIN phone account should be completed within 48 hours of reception, unless the prisoner is received during non-operational hours in which case the process should be completed within 48 hours of operational hours commencing.

9.7 A permitted exception to section 9.6 requires prisoners to be given access to a telephone on the first night in Reception, if available, or else in the first night location, in line with paragraph 2.42 of *PSI 07/2015 – Early Days in Custody*. Governors must ensure that robust and compliant local arrangements are in place to facilitate such calls. Consideration must be given to risk:

- For newly arrived prisoners' reception staff must read the Prisoner Escort Record and the police/CPS MG6 to identify whether any restrictions need to be placed on the prisoner's communications. In addition, if the prisoner is subject to (or likely to be subject to) public protection restrictions, or is provisional category A/category A prisoner, a member of staff must make the call on the prisoner's behalf, checking that the recipient is willing to receive the call in the first instance.
- For prisoners transferring in from another establishment, their PIN phone account will already be active, however staff must also consider any information or intelligence included within the transfer handover that may be relevant to the consideration of restrictions.

Staff must also check the alerts on the prisoner information system for active restriction of contact. Any identified restrictions need to be applied and managed in line with section 6 of this Policy Framework.

9.8 If a prisoner wishes to make a legal or confidential call before the process in section 9.6 has taken place, a decision must be made by the duty governor as to whether the call can be granted and only allowed in exceptional circumstances. If the duty governor grants a call, staff must undertake the checks outlined in section 11.6 before the prisoner is allowed to make the call using an official telephone.[17]

9.9 Governors and senior managers/AOs must ensure that prisoners subject to live monitoring can make telecommunication calls when live monitoring can be achieved. Governors must ensure that provision for live monitoring is prioritised within the LSS.

[17]Prison landline telephone

9.10 Prisoners must not be allowed to use the internet, other than for educational or resettlement purposes, or, where appropriate, to receive downloaded information for those purposes. This includes access and/or contributing via third party to social media content whilst in custody. Preventing prisoners from accessing the internet (including social-networking sites) is necessary to prevent communication with the public which circumvents restrictions outlined in Prison Rule 34(1)/YOI Rule 9(1) that prevent potential serious harm. In addition, uncontrolled access to the internet may allow the accessing of content that enables further criminality or otherwise impact on the security of the estate and/or public safety. Such restrictions are proportionate as controlled access for specific purposes is permitted.

9.11 For prisoners within category D/open prisoners, paragraph 9.10 applies in relation to systems approved by HMPPS for internet use, and on a restricted access basis. Outside of the estate, the prisoner's ROTL licence will determine what restrictions are applied to the prisoner in terms of their access/use of the internet and online activity.

The Interception of Prisoner Communications

10.1 Under Prison Rule 35A(1)/ YOI Rule 11(1), the Secretary of State may give directions to any governor concerning the interception in a prison of any communication by any prisoner or class of prisoners if the Secretary of State considers that the directions are necessary on the following grounds:

a) the interests of national security;
b) the prevention, detection, investigation or prosecution of crime;
c) the interests of public safety;
d) securing or maintaining prison security or good order and discipline in prison;
e) the protection of health or morals; or
f) the protection of the rights and freedoms of any person[18],
and in all cases proportionate to what is sought to be achieved.

10.2 In addition, under Prison Rule 35A(2)/YOI Rule 11(1) the governor may make arrangements for any communication by a prisoner or class of prisoners to be intercepted in a prison by an officer or an employee of the prison authorised by the governor if he considers that the arrangements are necessary on the following grounds:

a) the interests of national security;
b) the prevention, detection, investigation or prosecution of crime;
c) the interests of public safety;
d) securing or maintaining prison security or good order and discipline in prison;
e) the protection of health or morals; or
f) the protection of the rights and freedoms of any person[19],
and in all cases proportionate to what is sought to be achieved.

10.3 However, Prison Rule 35A(2A)/YOI Rule 11(2A) provides that the governor may not make arrangements for interception of any communication between a prisoner and:

a) the prisoner's legal advisor, or

[18] Any reference to the grounds specified in paragraph (4) above in relation to the interception of a communication by means of a telecommunications system in a prison, or the disclosure or retention of intercepted material from such a communication, shall be taken to be a reference to those grounds with the omission of sub-paragraph (f).
[19] Any reference to the grounds specified in paragraph (4) above in relation to the interception of a communication by means of a telecommunications system in a prison, or the disclosure or retention of intercepted material from such a communication, shall be taken to be a reference to those grounds with the omission of sub-paragraph (f).

b) any confidential access body as outlined in Annex B "Confidential Access List", unless the governor has reasonable cause to believe that the communication is being made with the intention of furthering a criminal purpose and unless authorised by the CEO of HMPPS or the director responsible for national operational services of that service, or the duty director of that service.

10.4 *PSI 49/2011 – Prisoner Communication Services* refers to the rights and entitlements for prisoners to communicate with those outside, including legal advisers, and must be followed. As current secure social video calling and prisoner email systems by their operating nature intercept correspondence, prisoners must not use these services for legally privileged and confidential access communications.

10.5 Rules on interception of communications apply equally to young people in custody (YOI Rules 9 – 15 mirror Prison Rules 34, 35, and 35 A-D). All establishments holding young people must have in place local instructions in line with this interception chapter and that take full account of the requirements of *PSI 08/2012- Caring for Young People in Custody*, to undertake monitoring where it is necessary and proportionate to do so, and to consider the greater impact of intrusion on this cohort.

Management of PIN Phone System

11.1 The PIN phone system is a private telecommunications system, and the interception of telephone calls takes place before the call connects to the public network. To provide adequate facilities to allow prisoners to maintain contact with others by telephone, the PIN phone system is configured to record all telephone calls that prisoners make, except those to legal advisers and organisations given confidential access (see Annex B "Confidential Access List").

11.2 In accordance with Prison Rule 35A(1)/YOI Rule 11(1), the blanket recording of social telecommunication calls is considered necessary on each of the grounds in Prison Rules 35A(4) to allow for the retrospective identification and management of attempts to abuse the PIN phone system. Illicit communications can facilitate a range of criminality in both prisons and the community and will also impact on prisoners' rehabilitative journeys. These communications cannot be identified in advance of being made because they can originate from any prisoner within the estate, and not solely those who are already subject to monitoring because of intelligence or risk assessments. Blanket interception also ensures that prisoners whose calls would otherwise not be intercepted are protected from coercive or threatening behaviour by those seeking to access their PIN-phone accounts. This is proportionate as prisoners and their social contacts are made aware that their calls are recorded and may be subject to monitoring. It is not however necessary to monitor most of these calls. In addition, prisoners sign the Annex C "Communications Compact" on reception (see section 12) and recipients of calls are made aware that the call is coming from a prison and will be recorded and potentially monitored.

11.3 Establishments must ensure that records of number checks and a full audit trail of decision making, and monitoring are recorded using the relevant forms and logs provided in Annexes 1-11 of the *Interception and Restriction of Communications Operations Manual*. These applications must be stored electronically and saved as an attachment on the prisoner's intelligence profile.

11.4 Establishment practice relating to the creation and allocation of PIN accounts, PIN phone access, call enabling regimes, and the size and amendment of a prisoner's personal list must be delivered in line with paragraph 6.13 of *PSI 49/2011 – Prisoner Communication Services.*

11.5 For the following cohorts, prison staff must ensure that social telephone numbers submitted for addition to a prisoner's PIN phone account are checked to ensure the recipient is who the prisoner purports them to be:

a) category A (including potential/provisional);
b) remanded or convicted of terrorism or terrorism-connected offences;
c) identified as posing a risk or a potential risk to children;
convicted or remanded for a harassment offence (including stalking) or subject to a court-imposed restriction or order, such as those as set out in the *Prison Public Protection Policy Framework*.
d) identified as a domestic abuse perpetrator, or where there is a domestic abuse protection notice issued, or domestic abuse protection order imposed;
e) cautioned, convicted, or otherwise dealt with in respect of a sexual offence listed in Schedule 3 of the Sex Offences Act 2003;
f) a risk involving the intimidation of victims/witnesses;
h) an E-list prisoner.

The checking of submitted social contacts for prisoners in cohorts outside of the above list is not mandatory and can therefore be considered and managed locally in consideration of risk and resource.

Contacts for prisoners subject to the ECV scheme or AVS must not be added unless they are on their respective contacts list or they are remitted discretionary contact in accordance with paragraphs 23.38 – 23.42. Additional conditions also apply for category A prisoners subject to AVS – please see *PSI 43/2014 Management and Security of Category A Prisoners*.

Once the social contact is verified, social numbers can be added to the PIN phone system, unless:

a) they are the prisoner's legal adviser or a confidential access organisation, in which case they must be added to the closed side of the PIN phone system subject to completion of the checks described in paragraph 11.6
b) they are identified as the victim of a prisoner and the decision is made in line with 2.26 of *PSI 49/2011 – Prisoner Communication Services*
c) intelligence suggests the submission of a number is an attempt to circumvent restrictions outlined in section 6.
d) intelligence suggests or there is a reasonable suspicion that the contact number is for another prisoner(s)

Checks must at least include confirmation of the identity of the person the staff member is speaking to, confirmation of how they know the prisoner in question, and identify whether the person is happy to be contacted by the prisoner on the number provided. Should any restrictions beyond preventing addition to the PIN phone account be considered necessary from these checks, then the application process outlined in section 6 of this Policy Framework must be followed. Where any suspicion emerges from these verification checks that the contact is not who the prisoner purports that they are, an Intelligence Report (IR) must be submitted.

11.6 In relation to submitted legal numbers, The Law Society, Bar Council and Chartered Institute of Legal Executives' websites can be used to confirm that the number and the person they purport to be are genuine. However, the number should still be contacted, and in cases where a mobile number is supplied staff should confirm, using open-source information during office hours, the number of the contact's office for additional validity checks. If a number relates to a foreign national or overseas legal professional, attempts must be made to verify using relevant online law registries and open-source internet checks. Confidential access numbers must be checked against the published list in Annex

B “Confidential Access List”, plus open-source internet checks and a phone call with the contact to confirm that the number is legitimate (and which should include the above process for confirming their office if the number is a mobile). Where any suspicion emerges from these verification checks that the contact is not who the prisoner purports that they are, an IR must be submitted and email sent to the CAB, highlighting the IR Unique Reference Number. Governors should consider whether any further action is required.

11.7 Where checks are undertaken on social contacts submitted by a prisoner under a category listed in 16.7, senior management must ensure certified translation providers that have a contract with HMPPS are utilised in the first instance in cases where a contact does not communicate in English – either an official translator who speaks the relevant language or automated translation where this is available. In the absence of either and as a final option, the governor may authorise volunteered staff who are able to sufficiently communicate in the language to undertake the checks.

11.8 When undertaking checks on submitted contacts, staff must, where possible, minimise delays in their addition to the prisoner’s PIN account. For example, if a list of numbers has been submitted by a prisoner, each number should be added to the account once checked, rather than waiting for every number on the list to be checked. Staff adding numbers on a case-by-case basis must, where possible, notify prisoners of each addition as soon as is practical. The *Interception and Restriction of Communications Operations Manual* provides further guidance on the process of checking submitted contacts.

11.9 Establishments must ensure that any restrictions to requests to add numbers are imposed only when necessary and proportionate in accordance with Prison Rule 34/YOI 9. Requests for the addition of 0800 numbers as social contacts, and numbers linked to call diversion and re-routing services, must be restricted under these grounds, as such numbers/platforms can facilitate diversion to certain contacts, circumventing restrictions that have been imposed and potentially causing serious harm. The *Interception and Restriction of Communications Operations Manual* provides further information on exceptions and managing breaches/offences.

Communications Compact

12.1 The Communications Compact (Annex C “Communications Compact”) ensures that prisoners are aware of their privileges with regards to telephone calls, secure and official video calls, letters, and emails. It also summarises the powers to intercept communications, and content that is not permissible during communications in line with paragraph 11.3 of *PSI 49/2011 – Prisoner Communication Services*. The Communications Compact must be discussed thoroughly with all prisoners upon initial reception and the document must be signed. Prisoners must be informed during this stage that their communications may be monitored and that their calls (other than calls to their legal adviser and confidential access organisations) will be recorded. The simplified version of the Communications Compact may be used as an aide to help prisoners understand the information. Staff must ensure there is local provision to support prisoners who may have difficulty in understanding the compact and its meaning (for example, due to language used, learning difficulties or age). The detailed version must be signed by the prisoner and kept in the prisoner’s security file and an electronic version should be kept on the prison I.T system. As part of the process the prisoner must be given sight of the current Annex B “Confidential Access list”. Annex B must be made routinely available to prisoners after the compact has been signed – for example, by providing prisoners with a copy, or by displaying copies in relevant locations within the prison.

12.2 It is only after the process outlined in 12.1 has been completed that the prisoner may provide a list of contacts for adding to the PIN phone system, which is to be undertaken in

line with *PSI 49/2011 – Prisoner Communication Services*. A maximum 20 social numbers and 15 legal numbers must be supplied using the application form in Annex 5 - "Application for Social and Legal/Confidential Contacts" in the *Interception and Restriction of Communications Operations Manual.* For AVS requirements, please refer to s*ection 4 of PSI 43/2014 Management and Security of Category A Prisoners*.

12.3 Prisoners have the right to refuse to sign the Communications Compact. In this instance, it must be explained that they will not be able to communicate via telephone calls, secure social video calls, letters and email until the Communications Compact is signed. This is necessary and proportionate in accordance with Prison Rule 34/YOI Rule 9 because the Communications Compact contains rules necessary to prevent prisoner communications being used to cause harm and ensures that the prisoner is aware that social telecommunications are recorded and that all communications may be subject to monitoring.

12.4 Should staff identify that a communication breaches the conditions of use set out in the Communications Compact, consideration must be given to whether the breach is serious enough to require reporting to a senior manager. Regardless, an IR must be submitted, detailing the breach and outcome of the decision to report. During live telecommunication calls, prison staff must consider whether the termination of the call is both necessary in accordance with Prison Rule 35A(3)/YOI Rule 11(3) and proportionate. If a call is terminated, this must be documented on the prison information system and in an IR, and the prisoner must be informed as to the reason why. Staff should also consider charging the prisoner with an offence under Prison Rule 51(23) YOI Rule 55(25) and, where there is evidence of a possible criminal offence, consider referral to the police in accordance with the *PSI 05/2018 - Prisoner Discipline Procedures (Adjudications)* and the *Crime in Prison Referral Agreement*.

12.5 During live secure social video calls communication may additionally be restricted by pausing the call, when necessary and proportionate in accordance with Prison Rule 35A (3)/ YOI Rule 11(3). The prisoner must be informed as to the reasons for the call being paused. Once a social video call has been ended by prison staff, it cannot be started again. Another social video call will need to be booked.

12.6 The signed Annex C “Communications Compact” (see section 12) may be produced in evidence at any subsequent adjudication.

Monitoring and Interception Protocol

13.1 The Secretary of State directs that all social telecommunication calls by prisoners on HMPPS systems authorised for this use[20] are recorded. This direction does not extend to social telecommunication calls made on personal mobile phones. The blanket recording of social telecommunication calls is considered necessary on each of the grounds in Prison Rules 35A(4)/ YOI Rule 11(4) to allow for the retrospective identification and management of attempts to abuse the PIN phone system. Illicit communications can facilitate a range of criminality in both prisons and the community and will also impact on prisoners’ rehabilitative journeys. These communications cannot be identified in advance

[20] This includes systems that use the PIN phone (and equivalent) system and secure social video calling platforms.

of being made because they can originate from any prisoner within the estate, and not solely those who are already subject to monitoring because of intelligence or risk assessments. Blanket interception also ensures that prisoners whose calls would otherwise not be intercepted are protected from coercive or threatening behaviour by those seeking to access their PIN-phone accounts. The blanket recording of social telecommunication calls is considered proportionate because prisoners and their social contacts are made aware that their calls are recorded and may be subject to monitoring, the extent of which is determined by assessed risk. In addition, the monitoring of calls is subject to a necessity and proportionality assessment in accordance with this policy.

13.2 Monitoring can take place both during a call (live monitoring) and after a call has been made (retrospective monitoring). Certain prisoner cohorts will be initially subject to mandatory live monitoring (see section 17), however the governor or AO can also authorise live monitoring where necessary and proportionate following the process set out in paragraph 13.5, for example, where a threat to life risk has been identified.

13.3 After having been intercepted in a prison, calls that are recorded as per 13.1 will be stored in a central repository which can be accessed by regional and national intelligence staff. Any access by or disclosure of repository material beyond prison staff and Secretary of State officials must be authorised in accordance with Prison Rule 35C / YOI Rule 13. This repository will be operated in line with the requirements set out in the *Interception and Restriction of Communications Operations Manual*, which also contains further guidance and information on the subject.

13.4 Any monitoring of telecommunications stored in the central repository must only be carried out in an official HMPPS/ MOJ premises and headphones/earphones must be used at all times to prevent unauthorised persons overhearing conversations.

13.5 The following administrative tasks must be undertaken by staff to ensure that interception and monitoring activity is conducted in accordance with the law and this Policy Framework.

a) Annex 2 "Application for the Authorisation of the Monitoring of Communications" in the *Interception and Restriction of Communications Operations Manual*, must be completed and authorised before monitoring can be undertaken.
b) The exception to this in where an establishment is looking to implement the interception (copying) of written communications on a full/partial basis (see paras 14.3 – 14.8 of this policy framework) – in such cases Annex 3 – "The Application for the Interception and Copying of Correspondence" must instead be completed.
c) Governors and AOs must ensure that all grounds for monitoring, and any refusals of applications to monitor are documented on the application. For applications relating to those under the age of 18, consideration must be given to the likely greater impact this intrusion will have and the proportionality should take into account the age of the person it is being applied to.
d) Monitoring staff must electronically attach any applications and authorisations to monitor communications to the prisoner's profile on the prison intelligence system.
e) Monitoring staff, AOs and governors must ensure that the relevant sections of the Authorisation of Monitoring of Communications form are completed each time the activity is renewed, and that these are attached to the prisoner's profile on the prison intelligence system.
f) Category A and E-List prisoners subject to live monitoring must be informed on first reception into prison or when they become the relevant Category A or E-List (if later) if their communications will be monitored, and all prisoners must be informed of the potential for intelligence-led monitoring.
g) Any intelligence gained from monitoring that may be of interest to prison management or other Agencies must be submitted on an IR, in line with the

Intelligence Collection, Analysis and Dissemination Policy Framework, and documented on Annex 6 - "Individual Monitoring Log" of the *Interception and Restriction of Communications Operations Manual*. The intercepted material must be managed in line with the retention protocol in section 18.

h) The monitoring of telecommunications should only be undertaken for those calls made on HMPPS systems approved for that specific use. For example, this does not extend to calls and video calls made using personal mobile phones for those prisoners in Category D/Open prisons.

13.6 Monitoring activities can be undertaken by any staff member subject to the delegated authority outlined in 6.1 where time and resources permit. However, all staff engaged in monitoring must be locally assessed as competent in the undertaking of these duties by a manager and have a clear understanding of the specified grounds for monitoring, the purpose and scope of the authorisation, and the process for submitting intelligence.

13.7 Applications to monitor should only be submitted when the prisoner is situated within the establishment (for example, not during the act of a transfer or in hospital). The exception to this would be for applications to retrospectively monitor the communications of a prisoner who has been released. In these instances, the application should be authorised by the AO/governor of the releasing prison, however in exceptional circumstances NIU Band 8s can provide the authorisation.

13.8 When a prisoner who is subject to monitoring is transferred, it is the responsibility of the transferring prison to inform the receiving prison of this, and this should include relevant information to assist the receiving prison in assessing the necessity and proportionality of any ongoing monitoring. The receiving prison must apply the relevant monitoring requirements and processes in line with this policy framework; this will be dependent on the prisoner's cohort, or the type of monitoring undertaken by the transferring prison. The transferring prison must ensure that any open monitoring authority on a prisoner transferred out is closed and documented as such in line with the requirements of this policy framework. The post-transfer review or completion of other assessments not related to the communication controls within this policy framework should be considered in line with relevant national policy requirements.

13.9 The requirements outlined in paragraph 13.8 also apply when the prisoner being transferred has previously been subject to monitoring by the transferring prison, and that monitoring was terminated within 12 months prior to the date of transfer.

13.10 For secure social video call sessions, in addition to authorised monitoring activities outlined in this policy framework, a member of staff may observe all calls in the live stream concurrently, and on a visual-only basis unless suspicions concerning the behaviour of participants during a call arise. In accordance with Prison Rule 35A(1)/ YOI Rule 11(1), this direction of the Secretary of State is necessary on the grounds outlined in Prison Rule 35A(4)/YOI Rule 11(4) to maintain prison security, protection of the public, and prevention or detection of crime, as well as to enable the identification of breaches of secure social video calling rules (e.g. passing on of messages or unauthorised participants). The activity is proportionate as the staff member may listen to the audio feed for no longer than is required to confirm or disprove their suspicions and take further action if needed, and both prisoners and their contacts are aware that this activity will take place. Staff must keep a record of their reasoning why doing so is necessary and proportionate in an Individual Monitoring Log (IML) (see Annex 6 "Individual Monitoring Log" in the *Interception and Restriction of Communications Operations Manual*), when a call is monitored to confirm suspicions.

13.11 The observing member of staff may also focus on a specific secure social video call in the instance of a technical failure, and only if the prisoner and/or their contact agree to them viewing (and listening) to the call to help resolve this. An IML must be completed (see Annex 6 “Individual Monitoring Log” in the *Interception and Restriction of Communications Operations Manua*l) when a call is monitored to help resolve a technical issue. An IR must be submitted to document any breaches or intelligence identified in this manner.

13.12 Where required to investigate technical issues notified by either party to a secure social video call that are beyond the ability of prison staff to resolve, the supplier may view recordings of the call affected if all parties to the call consent. This will be limited to the extent required to resolve the issue.

13.13 Monitored calls conducted in a language other than English may be translated and transcribed during monitoring, if not already mandated due to the assessed risk of the prisoner in question. Calls transferred to the central repository will be automatically transcribed and, where necessary, translated if this has been requested as part of the application. The NIU must be consulted before any application is made to use the central repository automated translation and transcription resource.

13.14 Automated transcriptions and translations must not be used in isolation for evidentiary purposes, to make significant decisions which produce an adverse legal effect concerning the prisoner or significantly affecting the prisoner, or to store data (as a digital or hard copy) for longer than is permitted in this Policy Framework, the Data Protection Act 2018, and Prison Rule 35D/ YOI Rule 14. Transcripts must be reviewed by a manager for verification and action. Any decisions taken (for example, disclosure, dissemination, referrals or adjudications/other sanctions) must not be made solely on the results of automated technology, in accordance with section 49 of the Data Protection Act 2018. Transcriptions must be considered as intercepted material and thus subject to the retention, disclosure and dissemination processes outlined within this Policy Framework.

13.15 Some digital communication platforms in use within prisons (for example, prisoner email or prisoner messaging services) include automated keyword searching features. As the use of these constitutes monitoring, staff should not do so unless an application to monitor has been authorised for the communication/s in question.

13.16 If a communication is intercepted and/or monitored without authorisation (which includes instances of legally privileged numbers being added to the wrong side of the PIN phone system), then staff must ensure that any such unauthorised monitoring activity is terminated immediately, including any copies of the correspondence that are being produced, and that the Governor and/or AO is immediately notified.

13.17 For the purposes of this policy, unauthorised interception and/or monitoring is defined as:

a) The inadvertent interception (and any subsequent monitoring) of privileged (legal and confidential) communications without authorisation or otherwise in accordance with section 15 of this policy framework. This includes instances where a privileged number has been added in error onto the open side of the PIN phone system.

b) The monitoring of social communications without authorisation. This extends to the monitoring of a communication method that is not included within the scope of a completed monitoring application. For example, secure social video calls being monitored when the scope of the application only states telephone calls.

13.18 Once notified, the Governor and/or AO must ensure the following is undertaken:

a) Any existing recording or copy of the unauthorised intercepted material must be sealed in an evidence bag (downloaded onto DVD/CD where necessary) and stored in accordance with section 18 of this policy framework.

b) Any recorded material from privileged communications stored on the related communications system (for example, the PIN Phone system or PCMS) must be deleted.
c) If the relevant communication is identified to be legally privileged, ensure that, where necessary, the telephone number in question is moved to the closed side of the PIN phone system.
d) Undertake relevant checks to identify whether any other communications between the prisoner and the contact in question have been intercepted without authorisation, following the required actions in this section of the policy framework if identified.
e) An IR is submitted which sets out the circumstances of the unauthorised interception and the resulting actions undertaken.
f) Record the instance using Annex 8 "Unauthorised Interception and/or Monitoring Communications Report", in line with paragraph 13.16 of this policy framework.

13.19 Once Annex 8 "Unauthorised Intercepted and/or Monitoring Communications Report" has been updated, the Governor and/or AO must ensure that it is submitted to the CAB. The process of recording and submitting to CAB must be undertaken within 24 hours of the unauthorised interception being first identified.

13.20 The CAB will review submitted copies of Annex 8 "Unauthorised Interception and/or Monitoring Communications Report" and will provide a report of errors to IPCO every three months.

13.21 Any forms, logs, application forms or other documentation associated with the interception of communications must not be altered.

Written Correspondence (Letters and Emails)

14.1 The task of restricting (stopping) or intercepting (opening, reading or copying) written correspondence must be undertaken by trained staff in the mail facility, unless the governor makes the decision to utilise other staffing groups (e.g., to manage available resources). However, local training and/or guidance should be provided to any member of staff who may handle privileged communications (Rule 39 / YOI Rule 17 and Confidential Access) as part of their duties.

14.2 Where an application to restrict communications in accordance with Prison Rule 35A(3)/ YOI Rule 11(3) on the grounds in Prison Rule 35A(4)/ YOI Rule 11(4) has been made, communications including mail and email may be stopped from reaching the prisoner or being sent out.

14.3 Should an establishment identify that it is necessary and proportionate to intercept all (100%) written correspondence at that establishment, and the process outlined in paragraph 13.5 has been followed, then the governor must ensure that all prisoners (including prisoners who arrive during the period of monitoring activity) are made aware that, further to the terms and conditions of the Communications Compact, written communications to/from the establishment *will* be monitored and the handling and management of original copies may alter in line with paragraph 14.7 of this policy framework. Once the activity has ceased, prisoners must be again notified of the change.

14.4 All incoming and outgoing letters or emails that are read must be recorded formally on the appropriate electronic log in Annex 6 "Individual Monitoring Log (IML) and Annex 11 "Email Correspondence Log" *in the Interception and Restriction of Communications Operations Manual*.

Copying Written Correspondence

14.5 Written or email correspondence must not be copied unless deemed necessary and proportionate, in line with Prison Rule 35A(2) / YOI Rule 11(2A), and the governor or AO must formalise the decision in writing and store this electronically for audit purposes. Circumstances whereby written correspondence can be copied include the following:

a) To disclose to the Police or an internal or external team/agency (where disclosure is permitted in accordance with Prison Rule 35C/ YOI Rule 13).
b) Where a letter is to be copied as part of the Parole Dossier where it is relevant to the risk factors under consideration (where disclosure is permitted in accordance with Prison Rule 35C/ YOI Rule 13).
c) Where there is authority to intercept written correspondence which needs to be translated.
d) Where there is authority to intercept written correspondence and the letter may be relevant to a Prison and Probation Ombudsman's (PPO) death in custody investigation or another investigation (where disclosure is permitted in accordance with Prison Rule 35C/ YOI Rule 13).
e) Where an establishment, in line the Use of Narcotics Trace Detection Equipment on Correspondence Policy Framework, determines that the photocopying of written correspondence is required to prevent the conveyancing of illicit substances(see paragraph 14.6 for further instructions when this circumstance applies).
f) Where advice is required from the Prison Group Director (PGD) or another part of HMPPS, and in order not to delay receipt of the letter unduly, a copy is taken and attached to the request for advice.
g) If the volume of written correspondence being monitored exceeds staffing commitment at the time the letter is received.

Photocopying mail that contains personal data must be undertaken in line with the General Data Protection Regulation (Regulation EU 2016/679) and Data Protection Act 2018

14.6 Where an establishment determines, in line with the Use of Narcotics Trace Detection Equipment on Correspondence Policy Framework, that the photocopying of social correspondence is required to prevent the conveyancing of illicit substances, then this can be considered for application to:

a) Individual items of correspondence that have provided a positive indication which, when assessed alongside the wider intelligence picture, suggests that the prisoner may be involved in this route of conveyance, or
b) All (100%) of social correspondence to prisoners in the establishment.

In both cases, the process for intercepting and monitoring communications outlined in paragraph 13.5 must be followed. Where Annex A "Risk Assessment: Conveyance of Illicit Items Via Correspondence" in the *Use of Narcotics Trace Detection Equipment on Correspondence Policy Framework* has been completed in support of determining actions to prevent the conveyancing of illicit substances via social correspondence, then this may be attached or otherwise retained upon the completed Annex 3 "Application for the Interception and Copying of Correspondence". The interception authority will expire one month from the date of authorisation but can be renewed if it is considered necessary and proportionate to extend the period of activity. Renewals must be authorised by the last day of the existing period and documented on the aforementioned application. Interception activity can be cancelled before the end of the period, for example if there is a change in risk identified. The reasons for the cancellation must be documented in the relevant section of the application.

14.7 Should the photocopying of social correspondence be confirmed as necessary and proportionate, establishments should ensure that prisoners are notified. In addition, unless the original item received a positive reading from testing with drug trace equipment then prisoners must have the following options offered:

a) To give consent for the original item to be destroyed securely.
b) Returning of the original item to the sender.
c) Sending of original items to one single address (cost covered by prisoner).

Prisoners must have a 28 day period to respond, otherwise it will be assumed that they give consent for the item to be destroyed. Prisoners can request for an exception to be made, and for the originals to be provided. Such requests can be considered by Governors on a case-by-case basis; however, if deemed appropriate the item should be tested using drug trace detection equipment and in line with the *Use of Narcotics Trace Detection Equipment on Correspondence Policy Framework*.

14.8 Should the photocopying of social correspondence be confirmed as necessary and proportionate, establishments must consider any special adjustments made to incoming correspondence to meet the needs of the recipient such as those with visual impairments or learning difficulties. In the case of artwork or other items of mail in colour, this should include the considering of colour photocopies to retain a degree of authenticity.

Additional Handling and Opening of Written Correspondence

14.9 Establishments must ensure that outgoing mail to social contacts is submitted unsealed and appropriately labelled in line with the Communications Compact (section 12 outlines the process for legal and confidential mail). Prison Rule 35A(2)/YOI Rule 11(2) permits the opening of social mail where necessary and proportionate on the grounds in Prison Rule 35A(4)/YOI Rule 11(2). Governors and AOs must ensure that any instance of written correspondence being read as a result of such checks are recorded and retained using the form in Annex 6 “Individual Monitoring Log” in the *Interception and Restriction of Communications Operations Manual*. Para 2.31 of *PSI 49/2011 – Prisoner Communication Services* provides additional guidance that must be followed should incoming social mail be unmarked (no sender details on the envelope).

14.10 When a prisoner has been prevented from writing to a person or an organisation, communication with any other person at the same address will also be stopped unless the other person is classed as a close relative. In these circumstances, governors and AOs may wish to assess whether it is necessary and proportionate in accordance with Prison Rule 35A(2)/YOI Rule 11(2), to authorise monitoring on these communications to establish whether any risks exist. For further guidance, see the Communications Action Decision Process, in sections 3 and 4 in the *Authorised Communications Controls Detailed Guidance* and the corresponding section of the *Interception and Restriction of Communications Operations* Manual.

14.11 Social correspondence received for an ex-prisoner, which arrives after they have been released from custody, must not be opened unless staff are not sure who it is addressed to. Any such correspondence must be forwarded to the individual concerned in a plain envelope to their private address but if this is not known and they were released under the supervision of a relevant probation provider, it should be forwarded to their Supervising Officer to pass on. Failing this, correspondence should be placed back into the postal system/returned to the Post Office. Rule 39 and confidential post must not be opened to identify the addressee – in these circumstances the correspondence should just be placed back into the postal system/returned to the Post Office.

14.12 Any social correspondence which is addressed to a prisoner and received while that prisoner is unlawfully at large may be opened and read, with such activity considered necessary and proportionate in the interests of public safety and the prevention, detection, investigation or prosecution of crime in accordance with Prison Rule 35A(1)/YOI Rule 11(1). Legal and confidential mail addressed to a prisoner and received while that prisoner is unlawfully at large may be opened, read, examined and copied if the governor has reasonable cause to believe that it contains an illicit enclosure or that its contents endanger prison security or the safety of others or are otherwise of a criminal nature. All mail opened and read on such occasions must be appropriately recorded in accordance with section 14.4. If it is from a prohibited correspondent, it should be recorded as a case note on the prison information system and an IR submitted. Otherwise, it must be returned to the sender with a covering letter stating that the prisoner is no longer in prison custody and their whereabouts are unknown. If the sender's address is unknown and cannot be found, it must be stored in the prisoner's property.

Privileged Communications: Legal and Confidential

15.1 The definition and handling arrangements of correspondence under Prison Rule 39/YOI Rule 17 (legally privileged material delivered to or received from the prisoner's legal advisor or any court, either by post or legal visit under Prison Rule 38/YOI Rule 16) and the list of organisations/individuals to which Rule 39/YOI Rule 17 handling arrangements apply, is in *PSI 49/2011- Prisoner Communication Services. Communications* by these organisations/individuals outside of the definition in this paragraph are afforded similar protections in accordance with Prison Rule 35A(2A)/ YOI Rule 11(2A).

15.2 The list of organisations, persons and bodies subject to confidential access handling arrangements is in Annex B "Confidential Access List". Confidential Access correspondence is afforded the same privileged handling arrangements as Prison Rule 39/YOI Rule 17 correspondence, and other forms of communication (e.g. a telecommunications call) between a prisoner and those listed in Annex B "Confidential Access List" are afforded the same protections as Prison Rule 35A(2A)/YOI Rule 11(2A). Should an individual or organisation make contact to request their addition to the confidential access list, they must be directed to the NIU Policy and Projects Team who will manage the application process and update the confidential access list where required.

15.3 In accordance with Prison Rule 39(2)/YOI Rule 17(2), Rule 39 material may be opened if the governor has reasonable cause to believe that it contains an illicit enclosure, and the enclosure must be dealt with in accordance with the Prison Rules. In accordance with Prison Rule 39(3)/YOI Rule 17(3), Rule 39 material may be opened, read and stopped if the governor has reasonable cause to believe its contents endanger prison security or the safety of others or are otherwise of a criminal nature. Any correspondence between a prisoner and their legal adviser or organisations given confidential access status must only be opened in the presence of the prisoner concerned (unless he or she declines the opportunity), and the prisoner must be informed if such correspondence is to be read or stopped. The interception must be recorded on the relevant log in Annex 7 "Intercepted Privileged Telecommunications and Mail Log" in the *Interception and Restriction of Communications Operations Manual.* The *Use of Narcotics Trace Detection Equipment on Correspondence Policy Framework* outlines the instructions for testing legally privileged communications.

15.4 Any correspondence between a prisoner and their legal adviser or organisations given confidential access that is opened by prison staff, when not externally identifiable as such, must be managed in line with paragraphs 13.16 – 13.19, regardless of whether the contents are read or not. This includes instances where correspondence is opened due

to a reasonable suspicion that it is not from a legal adviser or organisations given confidential access status but on initial examination, it appears to be legitimate. Reading of the correspondence must not extend beyond identifying its bone fides as legally privileged, and the placed back in the envelope and passed to the prisoner. In addition, a letter must be sent to the sender, explaining the reason for the breach.

15.5 *PSI 49/2011 – Prisoner Communication Services* provides additional guidance that should be followed on the general handling and markings of legally privileged and confidential correspondence.

15.6 In accordance with Prison Rule 35A(2A)/YOI Rule 11(2A), the governor may not make arrangements for the interception of any other communications between a prisoner and their legal adviser, or organisations given confidential access status, unless the governor has reasonable cause (for example, intelligence of sufficient reliability) to believe the communication is being made with the intention of furthering a criminal purpose, and unless authorised by the Director-General or CEO of HMPPS (or designated deputy if unavailable). HMPPS staff must ensure that advice is sought from the CAB regarding applications and the governor or AO must support any application made. Annex 4 "Application to Intercept Legal/Confidential Telecommunications" in the *Interception and Restriction of Communications Operations Manual* must be completed and emailed to the CAB for their consideration. The applicant must ensure that the process for monitoring is followed in the event that the application is authorised, and that an auditable log of applications and responses is retained. The only grounds for authorising ongoing interception would be a reasonable belief that the continued communication is being made with the intention of furthering a criminal purpose. A central record will be updated by CAB.

15.7 Should the monitoring of a telecommunications call identify that the content is either legally privileged or from an organisation granted confidential access (for example, should a contact number have been incorrectly added to the social contacts side of the PIN account), then the process outlined in paragraphs 13.16 – 13.19 must be followed.

Types of Monitoring

16.1 The extent to which a prisoner's communications are subject to monitoring will depend on the risk and threat posed by them. Sections 16.2 – 16.15 outline the types of monitoring that may be undertaken within an establishment beyond that which is required by prisoner category (see section 17) and are applicable to all types of communications (excluding visits), with the exception of legally privileged and confidential access communications. All types of monitoring (except for Random Monitoring where a decision is recorded as per section 16.9) require an application to be completed and authorised before monitoring can be undertaken, as per paragraph 13.5(a).

Intelligence-Led Monitoring (ILM)

16.2 Intelligence-Led Monitoring (ILM) requires written authorisation and must be necessary and proportionate on one of the grounds cited in Prison Rule 35A(4)/YOI Rule 11(4). ILM requires use of the form at Annex 6, "Individual Monitoring Log (IML)" in the *Interception and Restriction of Communications Operations Manual,* as per section 13.5(f).

16.3 The monitoring authority will expire one month from the date of authorisation but can be renewed for additional periods if it is considered necessary and proportionate to extend the period of activity for one or more reasons listed in Prison Rule 35A(4)/YOI Rule 11(4). Renewals must be authorised by the last day of the existing period and documented on the application, and each renewal extends the authority for one month. However, should the monitoring cease to be necessary and proportionate during a period of monitoring, it

should be documented as such and cancelled immediately. It is essential that staff develop an intelligence profile of the subject(s) to assist the review process for ILM.

Immediate Response Monitoring (IRM)

16.4 Immediate Response Monitoring (IRM) may be initiated in circumstances where monitoring and interception is required to test intelligence. IRM requires written authorisation and must be necessary and proportionate on one of the grounds cited in Prison Rule 35A(4)/YOI Rule 11(4). IRM requires use of the form at Annex 6, "Individual Monitoring Log (IML)" in the *Interception and Restriction of Communications Operations Manual* as per section 13.5(f).

16.5 Initial IRM should be undertaken for a period of no more than five days before significant dates suggested within the intelligence and, where necessary, five days after; considering the necessity and proportionality for the outcomes being sought, details for reasons to monitor certain dates must be stated on the monitoring log. For any further monitoring required after this period, the process for authorising Intelligence-Led monitoring must be followed, as per section 16.2 – 16.3.

16.6 Should IRM be identified as necessary and proportionate, but there are limitations in available resources for the approval of an application (for example, during out of hours periods where there are no AOs on duty), then interim approval by the Duty Governor will be sufficient to commence monitoring. This must be confirmed in an email, and an application must be completed and authorised within 72 hours. The Duty Governor's email must be electronically retained alongside the application, and the application itself should reference that an interim approval was sought and outline the reasons why.

16.7 Establishments should ensure that no more than two periods of IRM are undertaken on the same prisoner within a single month, and that in each instance of monitoring the requirements of 16.5 are met. If the Governor or AO becomes aware of IRM applications made against a prisoner that exceed two periods of IRM a month, then a review must be undertaken to identify whether another type of monitoring – for example, ILM – is more proportionate.

Offence Related Monitoring (ORM)

16.8 The oversight of prisoners subject to the provisions of the *Prison Public Protection Policy Framework* is under the remit of the establishment's Offender Management Unit (OMU) or similar. The governor must formalise a process within the Local Security Strategy (LSS) whereby the OMU and Security department collaboratively share information and assess threats posed by these prisoners.

16.9 Monitoring must be considered on first entry to prison or on the prisoner gaining the relevant status for the following cases:

a) Identified as posing a risk or a potential risk to children
b) Convicted or remanded for a harassment offence (including stalking) or court order as set out in *the Prison Public Protection Policy Framework*
c) Identified as a domestic abuse perpetrator or potential perpetrator
d) Convicted currently, or in the past, of stalking
e) Cautioned, convicted, or otherwise dealt with in respect of a sexual offence listed in Schedule 3 of the Sex Offences Act 2003
f) A risk involving the intimidation of victims/witnesses

Consideration should include an assessment of risk, and whether the monitoring is necessary and proportionate on one of the grounds cited in Prison Rule 35A(4)/YOI Rule 11(4). ORM requires use of the form at Annex 6, "Individual Monitoring Log (IML)" in the *Interception and Restriction of Communications Operations Manual* as per section 13.5(f). If a decision is made that monitoring is not necessary and proportionate, then the outcome must be electronically recorded on PNOMIS / DPS following the guidance outlined in the corresponding section of the *Interception and Restriction of Communications Operations Manual*. When considering monitoring applications and reviews, OMU AOs must record their considerations as to why monitoring is necessary and proportionate using the Application for Monitoring form at Annex 2 "Application for the Authorisation of the Monitoring of Communications" of the *Interception and Restriction of Communications Operations Manual*. The monitoring authority will expire one month from the date of authorisation but can be renewed for additional periods if it is considered necessary and proportionate to extend the period of activity for one or more reasons listed in Prison Rule 35A(4)/YOI Rule 11(4). Renewals must be authorised by the last day of the existing period and documented on the application, and each renewal extends the authority for one month. However, should the monitoring cease to be necessary and proportionate during a period of monitoring, it should be documented as such and cancelled immediately. It is essential that staff managing the prisoner develop a profile of the subject(s) and the risk they pose in order to assist the review process for ORM.

16.10 If a prisoner poses a risk outlined in section 16.9 and has been transferred from another establishment, the receiving prison must check if monitoring was active at the previous establishment. If the AO considers that monitoring is still necessary and proportionate, then a new application for monitoring must be completed.

Random Monitoring

16.11 If the governor is satisfied that all other aspects relating to monitoring and interception are resourced and working effectively, a decision may be taken to opt-in to random monitoring. Any such decision must be recorded electronically and kept for audit trail purposes.

16.12 Random monitoring is determined as being proportionate and necessary for securing or maintaining prison security or good order and discipline in prison, and to uncover new risks and threats, in line with Prison Rule 35A(1)/ YOI Rule 11(1). This is because prisoners who are not otherwise subject to monitoring may still communicate in ways that pose risks to prison security, public safety or the other grounds in Prison Rule 35A(4)/YOI Rule 11(4), and random monitoring allows prisons to identify these risks or threats, or prisoners of interest. Monitoring must be no more than 5% of social telephone, secure social video calls, social letters and emails made from the establishment each day and monitoring must be recorded on the relevant log in Annex 9 "Random Monitoring Log" in the *Interception and Restriction of Communications Operations Manual.*

16.13 To ensure the integrity of random monitoring, a list of random prisoners must be generated using the PIN phone system and used to direct the order of random monitoring. This list must be used for all types of communication monitored.

16.14 The initial period of random monitoring will expire three months from the date of the decision to opt in, but can be renewed if 16.11 still applies at the end of this period. Any extension for random monitoring must be recorded electronically and kept for audit trail purposes.

16.15 Prisoners should be informed that their communications may be randomly monitored during induction.

Cohort-Specific Monitoring

17.1 Prisoners are not required to communicate in English unless they are identified as Potential, Provisional, Exceptional or High-Risk Category A prisoners (whether convicted or unconvicted and held in any Category of prison*)* or are identified as E-List Heightened and are subject to live monitoring. In these circumstances, it is necessary and proportionate to require the prisoner to communicate in English because they have been assessed as posing an imminent risk of escape, harm or further criminality or the impact on security or public safety requires the prompt monitoring of communications, which may otherwise be delayed for translation. This requirement is also proportionate because AOs may authorise another language to be used by these prisoners, providing that protocol concerning translation provision (paragraphs 11.7, 13.13, and 13.14 of this Policy Framework) is followed. Members of staff within the establishment may be used to assist with translation, however certified translation providers that have a contract with HMPPS may be used for translation services. Establishments must ensure that a strategy outlined in the LSS is in place to manage any risk relating to the monitoring of prisoners communicating in a language other than English.

17.2 Any secure social video calls made by E-List Heightened, High Risk Category A and Exceptional Risk Cat A prisoners must be live monitored by the supervising member of staff assigned as custodian of the laptop being used for the call. This is considered to be necessary and proportionate under Prison Rule 35A and YOI Rule 11(4) and relevant policies (*PSI 10/2015 and Information Security Policy Framework*) due to the identification of E-List Heightened prisoners posing a legitimate and sophisticated risk of escape, and High-Risk Category A prisoners as being either of significantly heightened risk of harm to the public or of notably high profile as a result of their index offence.

17.3 Establishments must ensure arrangements for monitoring the social communications of prisoners who fall under a category listed in paragraph 16.9 are stipulated in the LSS and are in line with both this Policy Framework and the contents of the *Interception and Restriction of Communications Operations Manual*.

17.4 Monitoring of social communications must initially commence for all prisoners who are categorised as:

- Confirmed Category A/Restricted
- Potential Category A/Restricted
- Provisional Category A/Restricted
- High Risk Category A
- Exceptional Risk Category A

The monitoring authority will expire one month from the date of authorisation but can be renewed for additional periods if it is considered necessary and proportionate to extend the period of activity for one or more reasons listed in Prison Rule 35A(4)/YOI Rule 11(4). Renewals must be authorised by the last day of the existing period and documented on the application, and each renewal extends the authority for one month. Communications to/from legal advisers and confidential access organisations are exempt from the monitoring outlined, unless the activity is otherwise identified as necessary and proportionate and in line with section 15 of this policy framework. The process for applying for monitoring outlined in section 13 of this policy framework, including the use of relevant forms, must be followed in all cases before monitoring commences.

17.5 For Standard Risk Category A and E-list prisoners, there is no initial period of monitoring required. However, staff should consider the necessity and proportionality of such activity

on a case-by-case basis. If monitoring commences, then it must be subject to the provisions outlined in section 13, and the continued necessity and proportionality reviewed on a monthly basis. If the monitoring ceases to be necessary and proportionate, then it should be documented as such and cancelled immediately. This includes any monitoring considered for a sustained period following pre-escort monitoring undertaken in line with paragraph 17.20 of this policy framework.

17.6 If a prisoner is Category A *and* belongs to another cohort who might be subject to monitoring requirements (e.g. public protection), then the Category A monitoring requirements must supersede those of the other cohort.

Confirmed Category A / Restricted Prisoners

17.7 Confirmed Category A and restricted status classifications are defined in section 2 of *PSI 09/2015 The Identification, Initial Categorisation and Management of Potential and Provisional Category A / Restricted Status Prisoners* and the processes for monitoring and interception of each Cat A classification must be followed, even if the prisoner is located outside the Long-Term High Security Estate (LTHSE). In accordance with Prison Rule 35A(1)/YOI Rule 11(1) it is considered necessary and proportionate to commence monitoring because they have been assessed as posing an increased risk of harm, further criminality or impact on the security of the estate and/or public safety.

17.8 To ensure proportionality, all Category A / Restricted prisoners subject to live monitoring must be informed that their communications will be intercepted using the form in Annex E "Formal Notification of Live Monitoring".

Potential Category A / Restricted

17.9 All social communications (telecommunications and written communications) of potential Category A / Restricted prisoners must be monitored from the moment they are categorised/received as Provisional Category A / Restricted. In accordance with Prison Rule 35A(1)/YOI Rule 11(1) it is considered necessary and proportionate to commence monitoring because they have been assessed as posing an increased risk of harm, further criminality or impact on the security of the estate and/or public safety. This assessment of risk may change once a decision has been taken on the prisoner's Category A status.

17.10 To ensure proportionality, all potential Category A / Restricted status prisoners subject to live monitoring must be informed that their communications will be intercepted using the form in Annex E "Formal Notification of Live Monitoring". The AO for interception must inform monitoring staff whether all communications are to be subject to live monitoring or not. Live calls must be monitored within 24 hours of the call being made. All communications must have been monitored before a prisoner is transferred.

Provisional Category A / Restricted

17.11 All social communications (telecommunications and written communications) of Provisional Category A / Restricted prisoners must be monitored from the moment they are categorised/received as Provisional Category A / Restricted. In accordance with Prison Rule 35A(1)/YOI Rule 11(1) it is considered necessary and proportionate to commence monitoring because they have been assessed as posing an increased risk of harm, further criminality or impact on the security of the estate and/or public safety. This assessment of risk may change once a decision has been taken on the prisoner's Category A status.

17.12 To ensure proportionality, all Provisional Category A / Restricted prisoners subject to live monitoring must be informed that their communications will be intercepted using the form in Annex E "Formal Notification of Live Monitoring. The AO for interception must inform monitoring staff whether all communications are to be subject to live monitoring or not. Calls that are not live monitored must be monitored within 24 hours of the call being made. All communications must have been monitored before a prisoner is transferred.

High Risk Category A

17.13 All social communications (telecommunications and written communications) of High Risk Category A / Restricted Prisoners must be monitored from the moment in which they are categorised or received as high risk. In accordance with Prison Rule 35A(1)/YOI Rule 11(1) it is considered necessary and proportionate to commence monitoring because they have been assessed as posing an increased risk of harm, further criminality or impact on the security of the estate and/or public safety. Communications must be made in English unless the prisoner or social contact does not speak English. In such cases, the governor must first approve the use of a different language and have arrangements in place to ensure that all communications are translated within 48 hours of the call being made or the letter being received.

17.14 Communications made in English may be monitored live but must certainly be monitored within 24 hours of the telecommunication/video call being made or letter/email received.

Exceptional Risk Category A

17.15 All social communications (telecommunications and written communications) made by Exceptional Risk Category A prisoners are monitored from the moment in which they are categorised or received as exceptional risk. In accordance with Prison Rule 35A(1)/YOI Rule 11(1) it is considered necessary and proportionate to commence monitoring because they have been assessed as posing an increased risk of harm, further criminality or impact on the security of the estate and/or public safety. Communications must be made in English unless another language is permitted to be used by the governor, and arrangements are in place to ensure communications are translated at the time of the call being made. Written correspondence must be translated in accordance with paragraphs 11.7, 13.13, or 13.14 of this policy frameworks and read before the letter/email can be posted/passed to the prisoner.

17.16 Telephone and secure social video calls must be monitored live throughout the time the prisoner has this classification and is subject to monitoring. There must be contingencies in place to terminate the call where necessary and proportionate to do so under Prison Rule 35A(3)/YOI Rule 11(3).

17.17 Calls must be booked in advance and Exceptional Risk Category A prisoners must not be able to make calls outside of these arrangements. However, establishments must ensure that adherence to this process does not result in refusals to give Exceptional Risk Category A prisoners a decent level of family contact.

Standard Risk Category A / Restricted

17.18 Communications by Standard Risk Category A / Restricted must be considered for monitoring on an individual case basis where an assessment of risk confirms it is necessary and proportionate for one or more reasons listed in Prison Rule 35A (4)/YOI Rule 11(4), unless outlined elsewhere in this interception chapter.

17.19 Prisoners may communicate in the language of their choice, but communications in a language other than English, and which are subject to monitoring, must be dealt with in accordance with paragraphs 11.7, 13.13, or 13.14 of this Policy Framework.

Category A Prisoners - Escort

17.20 Separate to any monitoring authority (including decisions to not commence monitoring for Standard Risk Category A prisoners and decisions to terminate the monitoring of Category A prisoners), when a Category A prisoner is due to go on escort, communications monitoring can be undertaken for a period of no more than 72 hours prior to the date of escort. This activity is considered necessary and proportionate in accordance with Prison Rule 35A(1)/YOI Rule 11(1) because Category A prisoners have been assessed as posing an increased risk of harm, further criminality or impact on public safety when outside of the security of the estate. For these cases, the completed National Security Framework Escort Risk Assessment must state whether monitoring will be undertaken prior to escort and serves as the authorisation for activity undertaken within the 72 hour period. If the prisoner is not already subject to a monitoring authority, and intelligence obtained during pre-escort monitoring identifies a need to continue monitoring beyond the 72 hour period, then an application for ILM must be completed in line with sections 13 and 16 of this policy framework.

E-List Prisoners

17.21 In accordance with *PSI 10/2015 - Management and Security of Escape List (E-List) Prisoners*, all communications made by E-List prisoners must be considered for monitoring on an individual case basis where necessary and proportionate. In accordance with Prison Rule 35A(1)/YOI Rule 11(1) it may be necessary and proportionate to commence monitoring because those prisoners have been assessed as posing an imminent risk of escape and it is important to supervise them to ensure they are not planning an escape with people they are communicating with. Cases must be reviewed by the AO on at least a monthly basis to ensure the duration of monitoring is proportionate to the threat posed.

17.22 All calls made by E-List-Heightened prisoners must be live monitored and there must be contingencies in place to terminate the call where necessary and proportionate to do so under Prison Rule 35A(3)/YOI Rule 11(3). Calls made by E-List-Standard, and E-List-Escort may be subject to live or retrospective monitoring, however, calls must be monitored within 24 hours of the call being made. The frequency of monitoring of E-List-Standard and E-List-Escort is decided as part of the initial assessment for E-List and considered at each review. It is authorised on the E-List assessment form by the AO for the interception of communications. All monitoring undertaken must be recorded on an IML.

17.23 Where a prisoner is subject to live monitoring, they must be informed of this using the form in Annex E “Formal Notification of Live Monitoring”. All calls must be pre-booked. Where a prisoner is not subject to live monitoring, any recorded calls that have not been monitored must be listened to in advance of any planned escort and, in the event of an emergency escort, as soon as is practical.

Terrorist prisoners

17.24 The monitoring of terrorist prisoners who are also Category A must be undertaken in line with the requirements of their respective category outlined in sections 17.7– 17.20. For all other terrorist prisoners, monitoring must be considered on first entry to prison or on the prisoner gaining the relevant status and imposed if it is necessary and proportionate for intelligence-led monitoring to be undertaken, for one or more of the grounds listed in

Prison Rule 35A(4)/YOI Rule 11(4). This consideration must include an assessment of intelligence. If intelligence-led monitoring is confirmed, it must be carried out in line with the requirements outlined in sections 16.2 – 16.3. If a decision is made not to monitor, then the outcome must be electronically recorded on PNOMIS/DPS following the guidance outlined in the *Interception and Restriction of Communications Operations Manual.*

17.25 All decisions taken, including not to monitor and subsequent reviews, must be reported to NCTCCC. The NCTCCC will then maintain a national database for audit purposes. Governing governors can also request that monitoring support is provided by the NCTCCC. Regional Counter Terrorism Teams (Counter Terrorism Units in High Security Prisons) must be consulted prior to authorising social video calls for terrorist and **[REDACTED]**.

17.26 Prisoners who are identified as having connections or risks associated with extremism (for example, links to specific groups or movements), but who are not classified as a terrorist prisoner, should not be subject to the monitoring processes outlined in paragraphs 17.24 -17.25. In cases where monitoring is being considered for these prisoners, and paragraph 17.6 of this policy framework does not already apply, staff must follow the processes outlined for either Intelligence-Led Monitoring or Immediate Response Monitoring (whichever is more appropriate).

Retention / Disclosure / Dissemination

18.1 In accordance with Prison Rule 35C/ YOI Rule 13, the governor or AO may not disclose intercepted material to any person who is not an officer of a prison or of the Secretary of State or an employee of the prison authorised by the governor for the purposes of this rule, unless that person considers disclosure to be necessary on the grounds specified in Prison Rule 35A(4)/YOI Rule 11(4) and proportionate to the aim achieved by the disclosure, or:

a) In respect of intercepted material or material obtained by overt CCTV used during a visit if all parties to the communication or visit consent to the disclosure.
b) In the case of material retained in relation to Prison Rule 35B/ YOI Rule 12 (a permanent log of communications) the prisoner to whose communications the information arises gives consent.

18.2 In accordance with Prison Rule 35D/YOI Rule 14, intercepted material shall not be retained for a period longer than 3 months from the date of interception, unless the Governor or AO is satisfied continued retention is necessary on the grounds specified in Prison Rule 35A(4)/YOI Rule 11(4) and proportionate to the aim achieved by the retention. All intercepted social video call content will be stored on servers supplied by the social video calling provider and access to the content is controlled under an auditable process by the governor/director. Should the intercepted material be subject to an internal complaint procedure or investigation, or an investigation by the PPO, then it should be retained until such matters have concluded and any recommendations on the return of intercepted material (e.g., a letter) have been actioned.

18.3 This retention protocol also includes metadata[21] and any translations or transcriptions of communications, which must be considered as the content of intercepted material and retained/destroyed alongside the original data. In cases where copies of translations and

[21]Metadata is defined as the data providing information about one or more aspects of the data; it is used to summarize basic information about data which can make tracking and working with specific data easier. Metadata is information stored within a document that is not evident by just looking at the file.

transcriptions are attached to an IR, rather than summarised within one, these must still be subject to this retention protocol.

18.4 Where intercepted material is retained for longer than 3 months, the governor or AO must continue to review the continued retention, with the first review taking place within 3 months of the date of first retention. The justification for continued retention must be formalised in writing and retained electronically for audit purposes. Retention must immediately end if justification ceases to exist whether this is assessed at the review date or any other time.

18.5 There must be an auditable, electronic record of every call monitored or correspondence read that is stored securely on the prison information technology (I.T) system for monitoring staff to access and update. Where necessary and proportionate in accordance with Prison Rule 35C/ YOI Rule 13, local arrangements must be implemented to disclose relevant intercept material with the Police and other agencies and to facilitate access to intercepted material where an application for prison interception has been authorised. Such disclosure must be done in accordance with the *Intelligence Collection, Management and Dissemination in Prisons and Probation Policy Framework.*

18.6 All physical entities (for example, compact disc recordings or letters) collected for evidence purposes must be stringently handled, stored and destroyed in accordance with *PSI 08/2016 – Dealing with Evidence*.

18.7 The governor or AO must ensure that intercepted content retained for intelligence/evidential purposes is done so securely and handled as at least Official – Sensitive material under the Government Security Classification (GSC). The security of personal data and any disclosure must be delivered in line with the requirements of the Data Protection Act 2018, *PSI 04/2018 - Records, Information Management and Retention Policy* and the *Intelligence Collection, Management and Dissemination in Prisons and Probation Policy .*

18.8 The requirements outlined in 18.1 – 18.7 extends to correspondence both sent and received via prisoner email services, with dates of deletion recorded on the relevant log in Annex 11 “Email Correspondence Log” in the *Interception and Restriction of Communications Operations Manual.*

18.9 All paper records, including paper monitoring logs and social/legal number applications, must be stored in accordance with *PSI 04/2018 - Records, Information Management and Retention Policy*. Copies of the signed Annex C “Communications Compact” (see section 12) are to be kept with the prisoner’s security file and stored in accordance with *PSI 04/2018 - Records, Information Management and Retention Policy.*

18.10 All materials related to intercept that are obtained by Police and other law enforcement agencies are subject to local retention protocol from the date the material is received by the external agency.

Voluntary Disclosure

19.1 Voluntary disclosure must be authorised by the governor, director or AO (Band 7 or above), only where necessary and proportionate in accordance with Prison Rule 35C/ YOI Rule 13. As part of the consideration, assessment needs to be made regarding the reason for sharing the information, how it will be used and whether ongoing disclosure will be required to achieve the outcome sought.

19.2 Material shared as voluntary disclosure can be used by the receiving force in their own intelligence or evidential interests, or those of wider law enforcement, unless a prison senior manager enforces specific handling conditions. It is for this reason that all voluntary disclosure must be by way of a 5x5x5 dissemination form to provide an appropriate audit trail and handling conditions. Further information regarding dissemination and handling conditions must be sought from the *Intelligence Collection, Analysis and Dissemination Policy Framework.*

19.3 Disclosure should be via the AO and can be direct to the law enforcement agencies. The AO must maintain an electronic log of all voluntary disclosure (see Annex 10 "Voluntary Disclosure Log" in the *Interception and Restriction of Communications Operations Manual*).

19.4 Materials shared externally must be stringently handled in line with The Management and handling of Evidence Policy Framework.

19.5 All intercepted materials that are obtained by Police and other law enforcement agencies are subject to the relevant organisation's local destruction protocol from the date the material is received by the external organisation.

Law Enforcement Monitoring Applications

20.1 When processing law enforcement applications for prison staff to conduct monitoring, the governor or AO must assess the necessity and proportionality of the request in accordance with Prison Rule 35A/YOI Rule 11, as well as the necessity and proportionately of any disclosure under Prison Rule 35C/ YOI Rule 13. This should include considering all available information about the prisoner and the risk posed in order to make and assessment on the risk posed. The reasoning and justification of the request must be recorded on the relevant form.

Subject Access Requests

21.1 A prisoner may make a Subject Access Request (SAR) under the Data Protection Act 2018 (DPA) as set out in the *Information Requests Policy Framework*. The Offender SAR Team can provide further advice on this matter and must be consulted by contacting: data.access1@justice.gov.uk when a SAR is made.

Other Data Subject Requests

21.2 Other requests, such as requesting that data be deleted or restricted should be sent to dataprotection@justice.gov.uk for advice.

Compliance

22.1 In order to test compliance with interception requirements, governors must ensure that assurance checks using the form provided by CAB is completed on a regular basis, no less than twice in a calendar year. Use of this form will provide a spot check of the current situation and is strongly advised for use in preparation for inspections by HMIP, OSAG and IPCO. A copy of the most recent completed version of the form must also be made available on demand to the CAB within 24 hours. PGDs and Senior Contract Managers may also request this form to either be completed with 24 hours' notice, or request a copy of the most recent completed version.

22.2 In addition, officers approving interception of telecommunications must satisfy themselves using the systems and processes available to them that all calls monitored have the

appropriate paperwork in place, and that downloaded calls also have data retention paperwork in place. All paperwork must be made available on demand, within no more than 24 hours, to the governor or regional office, HMPPS Controller (and line management), CAB or IPCO.

The Enhanced Contact Vetting scheme

Background

23.1 There have been several terrorist attacks committed in the UK by offenders who were under HMPPS and one (Manchester Arena) where the perpetrator had had contact with a serving terrorist prisoner. The chair of the Manchester Arena Inquiry concluded that the serving terrorist prisoner had a radicalising influence over the perpetrator of that attack and that measures should be put in place to restrict prisoner visits and monitor prisoner communications to mitigate the outward terrorist risk that a prisoner may pose to the public. Data in recent years shows that the terrorist prisoner population has been increasing and we expect this to continue, which will increase the risk of outward radicalising from prisons. Taking into account this and the Manchester Arena context, it is necessary and proportionate to apply conditions to the contacts for certain prisoner groups, in accordance with Prison Rule 34 / YOI Rule 9[22] and Prison Rule 73/YOI Rule 77.

Overview of the Enhanced Contact Vetting (ECV) scheme

23.2 All terrorist prisoners and people on remand for a terrorism offence for offences described in s247A of the Criminal Justice Act 2003 ('CJA 2003') are subject to the ECV scheme, unless there are exceptional circumstances for them not to be. If judged to be necessary and proportionate, **[REDACTED]**.

23.3 People within scope of the ECV scheme are limited to a maximum of twenty social contacts and these contacts are subject to certain checks and approval before communication can begin, unless exceptions apply. The checks will be carried out by the Joint Extremism Unit and CT Policing. For someone who enters prison after the ECV scheme comes into force, communication between the in-scope person and a proposed contact is not permitted while the checks are ongoing, unless an exception applies. For someone in prison when the ECV scheme comes into force, communication is permitted until vetting is complete and any restrictions are implemented.

23.4 Changes to a person's list of contacts cannot be made more often than every three months. The checks carried out on a person's contacts will be reviewed every three years unless circumstances justify an earlier review.

23.5 Governing governors, or a delegated operational manager, are the decision-makers under the ECV scheme. They will be supported and advised by the ECV team based in the Joint Extremism Unit.

Application of the ECV scheme

23.6 The ECV scheme is designed to mitigate the outward terrorist risk posed by the following cohorts to their social contacts:

A. all prisoners serving a sentence that includes an offence described in s247A(2) CJA 2003 ('a qualifying sentence');

[22] Enhanced Contact Vetting does not apply to prisoners under 18 years old.

B. all prisoners on remand for terrorism offences described in s247A(2) CJA 2003; and
C. **[REDACTED]**.

The ECV scheme applies automatically to all prisoners in categories A and B, above, upon their entry into custody, unless there are exceptional reasons for it not to. The ECV scheme may apply, if judged to be necessary and proportionate to manage the outward terrorist risk, to prisoners in category C above.

23.7 For category A terrorist offenders, the ECV scheme does not replace the AVS scheme (AVS) and, where applicable, both schemes operate simultaneously. Further guidance and information on AVS and the management of category A prisoners can be found in PSI 43/2014 Management and Security of Category A Prisoners and PSI 09/2015 The Identification, Initial Categorisation and Management of Potential and Provisional Category A / Restricted Status Prisoners.

23.8 Restrictions under the ECV scheme apply to visits, telephone calls and video calls. A prisoner is allowed social visits, telephone calls and video calls with only those contacts on their approved contacts list.

23.9 Restrictions under the ECV scheme also apply to written communications, including email. A prisoner to whom ECV applies can only send and receive mail from social contacts on their approved contacts list.

23.10 Prisons must verify that the recipient of outgoing mail is on the prisoner's approved contacts list. Prisons should verify that the sender of incoming mail is on the prisoner's approved contacts list.

23.11 Governing governors must ensure that they have Local Security Strategy procedures in place to operate the ECV scheme.

Contacts exempt from the ECV scheme

23.12 The following people do not need to be approved through the ECV scheme before being allowed to contact prisoners:

Official contacts in accordance with the definition under official visitors at paragraph 3.11.

Children

- No children will be vetted under ECV. Governing governors must follow the child contact procedures set out in the *Prison Public Protection Policy Framework.*
- Children can contact in-scope prisoners subject to the consent of their legal guardian and in accordance with child contact procedures and public protection procedures set out in the *Prison Public Protection Policy Framework*.

Legal advisers, others involved in the prisoner's legal proceedings and confidential access contacts outlined in Annex B of this Policy Framework:

- The prisoner's legal adviser (whose identity must be checked, following the process in paragraph 9.3 of the *Interception and Restriction of Communications Operations Manual*) if contacting the prisoner in a professional capacity, and verified by the prison in accordance with visitor verification policy in the *Management of Security at Visits Policy Frameworks.*

- People contacting the prisoner in connection with legal proceedings (but only if the prisoner's legal adviser (whose identity has been checked and verified) confirms they are connected to the prisoners' legal proceedings).
- Confidential access bodies outlined in Annex B this Policy Framework.

23.13 All legal/confidential contacts must be processed in accordance with the prisoners Communication Compact using Annex C in this Policy Framework.

23.14 A list of prisoner contacts must be kept locally for prisoners to whom the ECV scheme applies. Visits by people connected with the prisoner's legal proceedings should be included, for example the prisoner's solicitor/barrister or the solicitor/barrister's representative.

23.15 The privacy notice at HM Prisons Visitors Privacy Notice must be provided to all prospective contacts. The ECV team must also provide further information as to how the scheme will operate when making first contact with prospective contacts.

Operation of the ECV scheme – Adding and removing contacts to contact list

23.16 Where a new terrorist prisoner or prisoner on remand for terrorism offences is received at an establishment, the ECV team will send an induction pack with information on the ECV scheme and relevant forms to the Prison Prevent Lead (PPL) and the security department (or counter terrorism unit (CTU) in the high security estate (HSE)). The PPL will share these documents with the prisoner. If the prisoner cannot read, staff must make the prisoner verbally aware of the contents. Staff must provide further informal explanation or a translation if this is needed.

23.17 Where a prisoner subject to the ECV scheme applies to have someone added to their contacts list, or replaced on their contact list at a later stage, an application must be sent to the security department (or CTU in the HSE) requesting those changes.

23.18 Once completed, the application requesting changes to the contacts list will be returned to the PPL who will then share it with the ECV team, the prison security department/CTU and the visits booking clerk, the PIN clerk and the correspondence team (as required).

23.19 The ECV team must provide all prospective social contacts with information on identity verification, ECV checks and how the process may affect them.

23.20 Where prospective contacts decline to engage in the ECV process, they must be advised by the ECV team that they are likely to be refused contact with the prisoner. The PPL must also inform the prisoner of their prospective contact's decision.

23.21 Where existing contacts are suspended pending the outcome of the ECV checks, the prison must ensure that this is recorded on the prisoner's Mercury record and, where possible, on the visitor booking system, on PNOMIS / DPS and PIN phone system. Relevant teams must also be informed of the decision to suspend communication.

23.22 Once the ECV team has received the personal information required to start the vetting process and the first ID verification check has been completed, the subsequent checks carried out by the ECV team and partners can take up to eight weeks. If those checks are not completed within those eight weeks, the establishment may choose to add prospective contacts to a prisoner's approved contacts list until a decision is taken that they should not be on the list of approved contacts, following completion of the checks. The establishment and Regional Counter Terrorism Team (RCTT) should consider whether a period of monitoring should be authorised and carried out to mitigate any risks to do with

the prisoner having contact with members of the public who have not been through the ECV process.

23.23 The ECV team must log the prisoner's details along with the requested contacts' details on a centralised logging system. The establishment must log and keep a local record. The ECV team will track the progress of each request to add a new contact through the verification and checks stages.

23.24 Once the ECV scheme is applied to a prisoner, they will remain subject to ECV conditions should they transfer while checks are taking place.

23.25 Where a prisoner wishes to remove a contact from their contact list, they must apply to their security department (or CTU in the HSE).

Verification of contacts and further checks

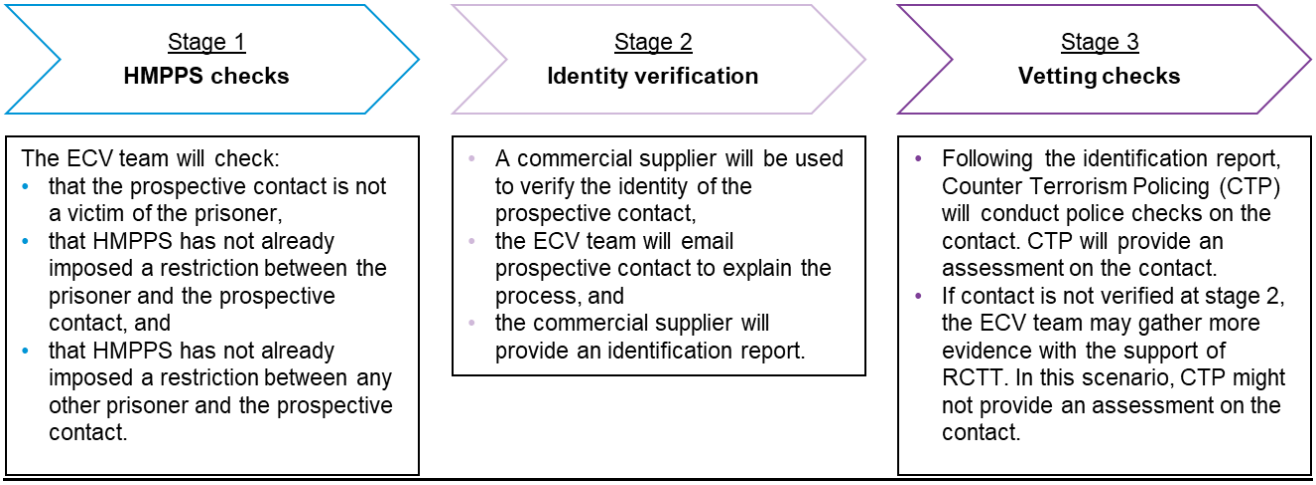
23.26 Checks will be carried out in the following three stages (see Figure 1 for a summary).

23.27 First, the ECV team will carry out internal HMPPS checks on the prisoner after they receive an application for someone to be added as a prisoner's contact. This stage includes checks that the prospective contact is not a victim of the prisoner, whether HMPPS has already imposed a communications restriction between the prisoner and the prospective contact and whether HMPPS has imposed a restriction on the prospective contact and any other prisoner. If a restriction is in place between the prisoner and the prospective contact, the verification process will stop and the PPL will be advised that the application will not proceed. If a restriction is in place between the prospective contact and another prisoner, the ECV team will gather and share with the RCTT more information about the restriction after the third stage of checks. If the ECV team is satisfied that the prospective contact is not a victim of the prisoner and that a restriction is not in place between the contact and the prisoner, the application will proceed to stage two.

23.28 Second, a commercial supplier will be used to verify the identity of the prospective contact. To do this, the ECV team will email the prospective contact to explain the ECV scheme and process and begin the verification process. If an email address for the contact has not been provided by the prisoner, the ECV team will attempt to contact the person to ask for their email address. An email address will need to be provided for checks to be carried out. If in exceptional circumstances this can't be done then decision-makers will need to take into account the fact that these checks could not be done. If the contact does not speak English, the ECV team may need to use an interpretation service.

23.29 Third, if the prospective contact's identification is verified at stage two then the report produced by the commercial supplier will be sent to Counter Terrorism Policing (CTP) so that it can conduct police checks on the contact. If the contact's identification cannot be verified at stage two, which might happen because the contact does not have the required identification documents, the ECV team may gather more information on the contact with the support of the RCTT and share this with CTP prior to checks. In this scenario, CTP might not be able to provide an assessment on the contact.

Figure 1 Summary of ECV vetting stages



Available actions following contact checks

23.30 Where a contact is assessed as presenting no concerns:

a) the ECV team must be informed and must log the outcome centrally;
b) the ECV team must communicate the outcome to the PPL and RCTT;
c) the PPL and RCTT must inform the establishment and prisoner that the contact can be added; and
d) the establishment and RCTT should consider whether a period of monitoring should be authorised.

23.31 Where a contact is assessed as presenting concerns:

a) the ECV team must be informed and must log the outcome centrally;
b) restrictions must be discussed and agreed at regional case management level;
c) the RCTT must inform the governing governor using a form of words;
d) the governing governor must make a decision whether to restrict the contact.

23.32 Where the governing governor, in discussion with the RCTT, decides that a contact must be restricted:

a) the ECV team must be informed and must log the outcome centrally;
b) the governing governor will receive a form completed by the ECV team and the PPL asking them to authorise the restriction, following the RCTT's advice;
c) the governing governor must complete and return the authorisation form to the ECV team;
d) the ECV team must communicate the outcome to the PPL and RCTT;
e) the PPL and RCTT must inform the establishment; the prison security department/CTU and the visits booking clerk, the PIN clerk and correspondence team (as required) that the contact is restricted;
f) the restriction must be retained locally and be recorded on PNOMIS / DPS; and
g) the ECV team must explain the governing governor's decision both to the prisoner and the prospective contact.

23.33 Where a contact is restricted, sufficient information must be disclosed to the prisoner to explain why it is necessary and proportionate to do so in accordance with Prison Rule 34/YOI Rule 9 and Prison Rule 73/YOI Rule 77. However, information can be withheld from disclosure to the prisoner if it is necessary for one of the following reasons:

- in the interests of national security;

- for the prevention, detection, investigation or prosecution of crime and disorder, including information relevant to prison security, good order and discipline;
- For the maintenance of prison security and good order and discipline in prison;
- for the protection of a third party who may be put at risk if the information is disclosed;
- if, on medical or psychiatric grounds, it is felt necessary to withhold information where the mental and/or physical health of the prisoner or a third party could be impaired;
- where the source of the information is a victim, and disclosure without their consent would breach any duty of confidence owed to that victim, or would generally prejudice the future supply or such information; and
- where disclosure is prohibited by law.

23.34 The prisoner must be advised of the appeal process via the prisoner request and complaint process. Appeals will be managed locally, with the support of RCTT where necessary and in line with the *Prisoner Complaints Policy Framework*.

23.35 All information must be stored, secured and handled in accordance with *PSI 04/2018 - Records, Information Management and Retention Policy*.

Contact limitations

23.36 Prisoners subject to the ECV scheme must have no more than 20 social contacts on their contact list. Contacts with multiple telephone numbers will only count as one social contact for the purposes of the ECV scheme. However, due to limitations with the PIN phone technology, each number will count as one contact on the PIN system and prisoners will still only be able to store 20 phone numbers at a time on the PIN system.

23.37 A prisoner subject to the ECV scheme may add to their contacts list until they reach a maximum of 20 contacts. It is only at this point that contacts may be substituted and once a substitution (or substitutions) has been made, further substitutions cannot be made for at least three months.

Discretionary contact

23.38 For prisoners subject to the ECV scheme who are in prison when the ECV scheme comes into force, current contact permissions must be maintained pending an ECV contact application, except where risks have been identified. Prisoners must complete and return their contact application form to the prison security department within four weeks of receiving it. Until ECV checks are complete, staff should be alert to any risks and consider monitoring of communications in accordance with sections of this policy framework. Where the governing governor deems it necessary and proportionate to mitigate identified risks, the contact will be restricted, in accordance with Prison Rules 34/YOI Rule 9 and Prison Rule 73/YOI Rule 77 , pending the outcome of their application. If the governing governor places a restriction on existing contacts in this scenario, both the prisoner and their contact must be notified and paragraph 23.32 must be followed.

23.39 For prisoners subject to the ECV scheme who enter prison *after* the scheme comes into force, while checks of contacts are ongoing governing governors may allow contact with close relatives (as defined by paragraph 3.12) and co-defendants (if communication with the latter relates to their conviction or sentence), unless it is necessary and proportionate

to not allow that communication on one or more on the grounds established in para 6.8. All other social and inter-prisoner contacts will be restricted.

23.40 For the duration of the vetting checks, establishments must verify all contacts locally before the prisoner is allowed to communicate with them.

23.41 Where discretionary contact is telephone or video call, the contact's identity must be verified (see paragraph 11.5 with respect to telephone calls) and an individual prisoner PIN account must be issued during induction into custody. Where discretionary contact is a visit, that must be a closed visit, pending the outcome of their ECV contact application. For visits, the contact must provide adequate means of identification on visiting, as outlined with the *Management of Security at Visits Policy Framework*. The governing governor must only allow discretionary visits once the initial application to add contacts has been completed by the prisoner and returned with suitable information, in accordance with paragraphs 23.16 – 23.18.

23.42 In exceptional circumstances, the governing governor may allow one-off communication between the prisoner who is subject to the ECV scheme and any other social contact who is not on the prisoner's contact list. RCTTs must be informed of any such decision by the governing governor and the communication should be supervised (e.g. a call should be monitored).

Interaction between the ECV scheme and Approved Visitor Scheme

23.43 For category A terrorist prisoners ECV does not replace the Approved Visitor Scheme (AVS) and, where applicable, both schemes will operate simultaneously. In order to avoid conflicting decisions on social visits, the governing governor, when considering restrictions under the ECV scheme, should take into account any decision made under the AVS.

Review Process

23.44 For convicted prisoners to whom the ECV scheme applies, a review (the "substantive review") of both the application of the ECV scheme and the prisoner's contact list must take place no later than three years after the decision to approve the first contact(s) to be added to the prisoner's contact list. The three-year deadline for the substantive review does not reset if changes are made to the contact list during that period.

23.45 First, the substantive review must consider whether the ECV scheme should still apply to the prisoner. For convicted terrorist prisoners (i.e. group A in paragraph 23.6) , staff must check the expiry date of the qualifying sentence(s). If it has not expired when the review is done, the ECV scheme will continue to apply to the prisoner unless there are exceptional circumstances for it not to apply any longer. For convicted prisoners where the qualifying sentence has expired and for all convicted prisoners to whom ECV has been applied on a discretionary basis (i.e. group C in paragraph 23.6), staff must consider in the substantive review whether it is necessary and proportionate for ECV to continue to apply.

23.46 Staff may become aware before the substantive review point that the qualifying sentence of a terrorist prisoner has expired (e.g. if the prisoner raises a complaint to say that their qualifying sentences have expired and they therefore must be reviewed). If this is the case, they must consider as soon as possible whether it is necessary and proportionate for the ECV scheme to continue to apply to the prisoner.

23.47 For prisoners on remand, the substantive review must be carried out at least every twelve months, starting from the date of the initial decision to approve contacts to be added to the prisoner's contact list.

23.48 Second, if it is decided that the ECV scheme will continue to apply to the prisoner, the prisoner's full contact list must be reviewed. This must involve renewal of checks carried out by partners to consider whether any approved contacts need to be restricted. It must also involve a reconsideration of decisions to not allow a contact to be added to a prisoner's contact list. Where a contact has been removed from a prisoner's contact list at the request of the prisoner and added again later, the vetting checks done on that contact do not need to be reviewed until the next substantive review.

23.49 Certain contacts might be reviewed on an ad hoc basis (the "ad hoc review"). For example, prisoners must notify the prison immediately if there is a change of circumstance (e.g. any criminal proceedings brought against a contact) to do with someone on their contact list, which might trigger a review of that contact. A review should also be considered where there is a reasonable suspicion (e.g. as a result of intelligence) that it is necessary and appropriate to put in place restrictions on a contact that has been approved in accordance with Prison Rule 34/Prison Rule 73/YOI Rule 9/YOI Rule 77 are satisfied. Any ad hoc reviews do not reset the time-limits for the substantive review, nor remove the need for a substantive review to be done.

23.50 The ECV team must generate (when initial action is taken), log and track the dates of substantive and ad hoc reviews on the centralised logging system for each contact. The ECV team must inform establishments of upcoming deadlines for a substantive review (i.e. the three-year deadlines for convicted prisoners and one-year deadlines for remand prisoners).

23.51 The ECV team must lead the substantive and ad hoc reviews and provide advice to governing governors for them to make any decisions that are needed. Where restrictions are recommended, the process outlined in paragraph 23.32 must be followed.

23.52 The prisoner must be informed of the date by which their substantive review must be carried out and that there might be reviews before this point for any of the reasons explained above.

Inter-prison communications

23.53 For prisoners subject to the ECV scheme, if they wish to contact a prisoner in a different prison, ECV checks must be considered, and approval must be sought in accordance with paragraph 6.7. If approved, they will be included in the prisoner's list of 20 contacts.

Safety

23.54 Prisoners, particularly those new to custody, may be vulnerable to violence or self-harm if social contact is delayed or not allowed under the ECV scheme. Staff should be alert to any signs that the prisoner's risk of harm to themselves or others has increased and support them appropriately. The case management processes described in the *Prison Safety Policy Framework*, such as Challenge, Support and Intervention Plan (CSIP) and Assessment, Care in Custody and Teamwork (ACCT) may, where appropriate, be useful to manage risk and contribute to prison safety. Further requirements, guidance and information about managing prisoner safety can be found in the *Prison Safety Policy Framework*.

Sanctions

24.1 Where breaches or attempted breaches of restrictions are identified, governors must consider appropriate sanctions in accordance with *PSI 05/2018 - Prisoner Discipline Procedures (Adjudications)*, and in the most serious of cases, referral to the police.

Criminal Offence

25.1 Where there is evidence of a possible criminal offence, the matter must be referred to the prison security and intelligence department for consideration of a referral to the police for investigation which must be dealt with in accordance with the Crime in Prison Referral Agreement. Where the possible criminal offence is committed by a terrorist or **[REDACTED]** prisoner, or the offence may potentially be terrorist in nature, the prison security and intelligence department should refer to the counter terrorism Annex to the Crime in Prison Referral Agreement.

Annexes

THESE FORMS ARE PUBLISHED SEPERATELY ON GOV.UK – LINKS BELOW

Annex A

Relevant form to be given to prisoner and the contact subject to communications restrictions.

- Official Notification to Contact Form
- Official Notification to Prisoner Form

Annex B

- **Confidential Access List**
  List of Confidential Access Organisations

Annex C

Communications Compact

To be signed by the prisoner upon reception. The simple version is to be used as an aide.

- Communication Compact – Detailed Overview
- Communication Compact – Simple Overview

Annex D

Intercepted Privileged Telecommunications and Mail Log

To be completed when any legal/confidential telecommunications are recorded and/or monitored in error or deliberate circumstances

- NSF Guidance on Inadvertent Capture of Confidential Information Mail
- NSF Guidance on Inadvertent Capture of Confidential Information Telecommunications

Annex E

- **Formal Notification of Live Monitoring:**

  A paper copy is to be given to the prisoner before live monitoring commences.