Emergency Compassionate Calls Protocol - iPads

April 2020

**Background**

HMPPS is making provision to supply establishments with two iPads to facilitate emergency compassionate face to face calls between residents and family members**.** Governors will decide what constitutes an emergencycompassionate need for the calls but these would normally be contact with a dying relative or possibly contact with a family member before or after a funeral.

The iPads have been enrolled onto a secure platform and can only be used for this purpose. Zoom has been installed onto the iPads to facilitate the calls and family members will need to have installed Zoom onto their smartphone or tablet.

The following bulletin details protocol regarding;

* Contacting family members
* Operational guidance
* Prisoner compact and expectations
* Risk management and compromise

# Enrolment and distribution of iPads

The iPads will be received by Regional Silver teams before being distributed to establishments. Regional teams will enrol the iPads onto the system and install Zoom prior to distribution. Guidance notes for enrolment have been sent separately.

Each iPad has it’s own DOM1 email address, Microsoft 365 user ID and password and Apple user ID and password. The guidance notes for enrolling each device must be followed sequentially to ensure that enrolment is sucessful. The Zoom account will need installing and registering using the guidance notes and 365 account details.

Asset registers have been supplied and will record which establishment each iPad has been distributed to, establishments must complete Annex A when the iPads are received.

This is a temporary solution for the duration of the current COVID19 crisis, all iPads will be collected and returned to Digital Justice at the end of the crisis period.

A template is provided (Annex C) for Governors to approve the iPads being brought into, and used in, establishments - Section 40E states that an authorisation can be given in relation to a particular prison either by the Secretary of State, by the governor/director, or by a person working in a prison who is authorised by the governor/director to grant the authorisation. As per section 40E(3), the authorisation must be in writing. The authorisation could be given to persons generally, or to specified persons, or persons of a specified description, and it may be given on such terms as may be specified in the authorisation.

A resident usage compact is attached at Annex B and must be signed before a call is made.

iPad cleaning advise is listed on Annex D (as per previous mobile phone cleaning advice).

# Operational guidance for use

iPads will only be used for emergency compassionate calls after the necessary application and approval is completed. The application (Visit to Dying Relative/Funeral Escort) must record comments from the following before being passed to the Governor or Deputy Governor for approval;

* Chaplaincy team – confirmation details on application form
* Security Department – known intelligence/security issues
* Police Intelligence/Liaison Officer - known intelligence/security /Police issues
* Offender Supervisor/Manager – information regarding recorded non-contact persons and any public protection issues

When a call has been approved by the Governor or Deputy Governor the following actions must be taken;

* Before a call can be made using the iPads a family member who will be present during the call must be contacted and informed of the call and need to download the Zoom app from an appropriate app store.
* The email address of the family member will be required to allow the establishment iPad to connect.
* To add a contact into the Zoom application the steps are as follows:
  + Click on the Zoom application (this will already be logged in as your establishment, if it is not, please speak with the SPOC within your establishment)
  + Click on contacts tab (left-hand side, fourth icon down)
  + Using the + sign (top right hand corner) > click Add a contact
  + Enter the recipient email address and click Add (an email will then be directly sent to the contact of which they will need to accept the contact invitation through the Zoom application)
  + Once the recipient has agreed to contact the iPad, within the Zoom application > contacts > external contacts > it will here show the email address previously added
* To make a call to the family members the steps are as follows:
  + Firstly ensure the contact has been added following the instructions above
  + Click on Zoom application
  + Click on contacts tab (left-hand side, fourth icon down)
  + Click on external contacts and there should be the contact information
  + Click on the email address > click meet > access to camera and microphone
  + Once the recipeint has accepted the request, it will come up on the screen as ‘JOE BLOGGS HAS ENTERED THE WAITING ROOM > click admit’

The following guidance and provisions must satisfied before the call can go ahead;

* A telephone call will be made to the family member prior to the video call to establish readiness and set expectations of behaviour during the call including;
  + Call must not be recorded
  + Confirmation that anybody listed as a non-contact person for the resident is not present
  + Appropriate language only
  + Prevention of other members of the public being filmed
  + Section 170 of the Data Protection Act makes it unlawful to obtain personal data without consent. It is an offence for a person knowingly or recklessly obtain, disclose or retain personal data. The following text should be read to the family member accepting the Zoom call.
    - “Please may I take this opportunity to advise you of the legal position whilst undertaking a Video Call, as we want to ensure you do not put yourself at risk of potentially being in breach of the Data Protection Act 2018. Her Majesty’s Prison and Probation Service (HMPPS), an executive agency of the Ministry of Justice (MoJ), does not consent to you retaining, sharing, or acting upon by any means, the information/conversation that you have received.  You could potentially be in breach of section 170 of the Data Protection Act 2018 if you disclose any of this information. This section states that it is an offence to, without the consent of the data controller, knowingly or recklessly obtain, disclose, or further retain personal data.”
* A suitable room for the call will be identified that affords some privacy for the call – iPads must not be taken into residential areas
* Supervising member of staff and a member of the Chaplaincy Team will be present at all times through out the call
* A log of the call will be completed and must include –
  + Name of person connected to
  + Mobile number/email address of person connected to
  + Duration of call
  + Any security information/issues raised during the call – an IR must also be submitted
* The supervising member of staff will initiate the call and pass the iPad to the resident when the call is connected
* The supervising member of staff must be vigilant to any security issues that might arise during the call including;
  + Indications the call is being recorded
  + Awareness of non-contact persons being present
  + Content of call that might represent a breach of security
  + Inappropriate behaviour/language
* The supervising member of staff must terminate the call if concerns are raised regarding the above points
* At the conclusion of the call all connection data must be removed from the iPad;
  + ‘End meeting’ will end the connection
  + To delete the information, go back to contacts > click on the email address that has just been contacted > top right hand corner click ‘**…**’ > Remove contact
  + This deletes the information and will not be stored within the application or any other parts of the device
* At the end of the call the iPad must be sanitised
* iPad must be returned to a secure location for storage – Governor’s/Deputy Governor’s/Head of Security’s safe

The continuation of this service relies on resident compliance and as such the requirements in the attached compact should be made clear (Annex B).

**Security, Risk Management and Compromise**

The use of iPads for emergency compassionate face to face contact presents an opportunity to continue to provide a safe, secure and decent prison environment under potentially difficult and challenging pandemic conditions. The use of these mobile devices are accompanied by a degree of risk that HMPPS has sought to mitigate and minimise.

The application and approval processes must be followed as per normal applications for dying relative and funeral applications. Use will be limited to residents with extenuating circumstances as confirmed by the Governor in the authorisation.

Safeguards are in place to prepare for the call and ensure that the security measures in place help to safeguard the family and wider community.

The iPad will be stored securely and under constant supervision and will be in line of sight all times. To reduce the risk of loss or compromise of the iPads they must not be taken onto residential units. Residents must not be left unsupervised when in possession of an iPad and a member of staff must be present throughout the whole video call, at a distance, for privacy.

Video calls will not be recorded.

Any incidents of loss, damage or operational compromise must be reported to Regional Silver as soon as possible.

ANNEX A

Establishment iPad Receipt Record

Establishments should label each mobile with the local ID code to enable the recording and reporting of mobile stock.

|  |  |  |  |
| --- | --- | --- | --- |
| **Local ID Code (Est code followed by BT001/2/3 etc)** | **Received by** | **Asset tag number** | **Storage location** |
|  |  | **K** |  |
|  |  | **K** |  |

**ANNEX B**

**Compact**

iPad Access Agreement

In order to support access to compassionate face to face calls in the event of a health and safety related ‘lockdown’ this establishment has made arrangements to offer an iPad to allow you to speak to family members in extenuating circumstances.

**If this service is misused access will to the iPad will be withdrawn.**

The iPad will be able to contact a family member via the Zoom video platform application (app)

**In signing this agreement you commit to;**

* using the iPad as directed
* use appropriate language during the call
* accepting that a member of staff will initiate the call and supervise for the duration
* hand the iPad back to the member of staff at the end of the call

Failure to follow these requirements will result in sanctions that may include use of IEP or adjudication.

Signed agreement:

|  |  |
| --- | --- |
| Resident Name |  |
| Resident No. |  |
| Location |  |
| Signature |  |
| Date |  |

ANNEX C

**Date:**

**Governor’s Name:**

**HMP**

**RE: AUTHORISATION OF iPAD & OTHER EQUIPMENT**

On behalf of the Secretary of State under Section 40E of the Prison Act I authorise:

1. The following List B Articles to be conveyed into HMP ; and

2. The transmission of sound and information using these articles from inside a prison for simultaneous reception outside the prison.

These authorisations are given in order to facilitate contact between prisoners, with no access to in-cell telephony, and their approved contacts listed in their prison PIN account - for the duration the COVID 19 emergency. This equipment will be used, stored and accounted for as per the operating model circulated separately.

**Mobile Phones**

|  |  |
| --- | --- |
| Model and asset tag no. : | No. of Devices: |
| **iPad – asset tag –K\_\_\_\_\_\_\_\_\_\_**  **iPad – asset tag –K\_\_\_\_\_\_\_\_\_\_** | **2** |

**SIM Cards**

|  |  |
| --- | --- |
| Service provider: | No. of SIM cards |
| **O2** | **2** |

*Section 40E states that an authorisation can be given in relation to a particular prison either by the Secretary of State, by the governor/director, or by a person working in a prison who is authorised by the governor/director to grant the authorisation. As per section 40E(3), the authorisation must be in writing. The authorisation could be given to persons generally, or to specified persons, or persons of a specified description, and it may be given on such terms as may be specified in the authorisation.*

**Signature:**

**Name:**

**Date:**

**ANNEX D**

**COVID 19: Mobile Phone Cleaning Guidance**

V1 Interim Live - HMPPS

Introduction

During periods of self-isolation, provision is being made for residents to access mobile phones to maintain contact with their families. It is essential that these phones are properly cleaned & disinfected after use to prevent unintended transfer of Covid-19.

Please find below the necessary list of materials and cleaning procedure; both are also appropriate for mobile phones shared by staff, e.g. driver or escort phones.

Materials Needed

• Small biohazard bag (yellow)

• Disposable nitrile gloves (blue)

• Small clear plastic bag (for the cleaned phone)

• Lint free / microfibre cloth

• Supply of 70% Isopropyl alcohol cleaning wipes (e.g. food probe wipes)

Procedure to Follow for Mobile Phone Cleaning;

• At all times, staff & residents must maintain good hand hygiene by way of frequent, thorough hand washing in line with PHE guidance.

• When issuing the phone to a resident, retrieving it after use and while cleaning the phone staff must wear disposable Nitrile gloves.

• Make sure the phone is unplugged before cleaning.

• Use a soft lint-free or microfibre cloth to remove any gross contamination. Dispose of the cloth into the yellow biohazard bag.

• Use a fresh cleaning wipe (70% Isopropyl alcohol - e.g. a food probe wipe or similar) to clean all faces of the phone gently but thoroughly, paying special attention to the whole of the front, the faces of any keys or buttons, and in between keys.

• Use more than one wipe if necessary. Allow to air dry.

• Place all used wipes into the same biohazard bag.

• Seal the phone into a new clear plastic bag ready for re-issue.

• Add your gloves to the hazard bag, seal, and dispose of according to local hazardous waste procedures.

