

OFFICIAL

Mobile Testing Unit Reference Information for host London Local Authorities

Mobile Testing Unit (MTU) and Regional Testing Centre (RTC) test bookings

MTU and RTC tests are by appointment only: Tests will only be conducted for those people who have an appointment booked via the national booking portal. Anyone without an appointment will be asked to book on-line before returning. This should also include any household members travelling if they expect to be tested.

Self-referral and employer referral registration links are on www.gov.uk/guidance/coronavirus-covid-19-getting-tested. The gov.uk page also includes details of who is eligible for tests.

Opening times for all MTU sites are approximately 10.30-15.30. As of 8 June some MTUs are now open until 16.00. Please see confirmation of times available when booking a time slot using the booking portal.

Access to tests at RTCs is for those in vehicles only. Tests at MTUs are available for those in vehicles and for pedestrians. Pedestrian access is technically possible but currently discouraged and registrations require vehicle registration details to be added when booking places.

Cleaning down after each pedestrian subject requires significantly more time and additional PPE to manage the site as well as clear segregation of pedestrian flow from the general public. It is intended to change this policy soon (to provide greater access for pedestrians) and the booking portal will be updated accordingly. We are aware of infection control concerns regarding pedestrians. This policy is set by DHSC and suitable infection control arrangements are in place at MTUs to manage pedestrian access.

Booking portal timings

30% of bookings are released 2 days in advance of the testing day. These are in part reserved for the employer referral booking system. The additional 70% are opened to self-referral bookings 1 day (at 20.00hrs) before the site opens.

The release of bookings onto the portal starts with employer referrals which have priority access from 17.00. The portal is set to allow self-referral bookings for the wider public from 20.00 onwards. At the same time 30% of the bookings for the following day (D+1) are opened on the portal.

Capacity fluctuates at sites according to the logistics of teams coming from a variety of hub locations (time constraint) and other resource constraints in the testing programme which are being actively managed.

Employer booking portal

Key worker employer organisations can register to use the employer referral booking portal (link to register [on this page](#)). The employer referral portal reserves a % of the test booking slots for employers to refer staff before those slots are released to the general eligible public via the self-referral portal. This system is more effective than it was at the start of the MTU testing capability because MTU locations are now available on the system further in advance.

The employer referral system enables employers to:

- Submit requests for test centre appointment allocations by uploading an excel file (.xls/.xlsx) each day.
- Download submitted requests which have had appointments allocated.
- View the status of your submitted requests each day after 5pm.

Employees will be sent a booking confirmation for their nearest test location with availability directly from the system.

OFFICIAL

As of 4 June, DHSC has moved the employer referral portal to a “continuous run” state. This means the original 3pm daily submission deadline has been removed. Employers will still upload only one spreadsheet a day, but all uploaded spreadsheets will be processed every 5 minutes between 8am and 6pm.

E.g. if an employer believes they are ready to upload requests at 11am they can upload then and it will be almost instantly processed. But if employers want to hang on past 3pm for any reason until later in the day, they can do so.

DHSC have also simplified the form to avoid errors that prevent employers from uploading successfully. E.g. they no longer ask for the vehicle registration number. DHSC have also added the user guide to the post-login page. All of this work is aimed at creating a more sustainable system.

Local Authority support

The military teams and MTUs are intended to be self-sufficient. They do require access to toilet facilities within proximity of the MTU location. In addition we recommend the following local authority support:

- Minimum of one local authority representative / liaison officer at the MTU during the scheduled hours of operation (10.00 to 16.00 but recommend available on site from 09.00 in case of early arrivals until close).
- Consideration of traffic management around the area of the site.
- Press officer available on-call if required e.g. in the event of media presence, MP or elected member visits to the site.

Some local authorities have also undertaken the following actions you may wish to consider.

- Deployed staff to offer advice to people in traffic queues (e.g. to inform people that no-one can be tested without a valid booking code)
- Deployed staff to provide additional security around the site location where considered useful.
- Provided temporary barriers/fencing to improve security.
- Provided food for the military personnel which has been very well received.

Liaison with the military

The MTU military team commander will usually make contact with the nominated site point of contact on the morning of the first day of the deployment. The assigned team receive the point of contact information as part of their deployment instructions each morning. If you do not hear from them, or from other military liaison officers in advance, we recommend the local authority point of contact for the day introduces themselves to the military team commander when they arrive on site. We recommend arriving on site at 09.00 although the arrival of the military team will vary depending on their travel time.

Public communications

The Cabinet Office and DHSC are working on further public communications advice. An MTU local comms package and FAQs (attached) have been provided. While you can use these documents to inform your comms, please do not share the documents outside your local authority.

When communicating with the public about the MTUs please:

- include a clear statement that no-one should turn up without an appointment. Those without a confirmed booking will not be able to be tested;

OFFICIAL

- do not publicise the location of the MTU. If publicising the MTU, only include a statement that it will be deployed in the Borough and full details are or will be available via the self-referral booking portal on gov.uk.

Data on the number of tests undertaken at MTUs (individual locations or collective) should not be released to the media. This data is owned by DHSC and is shared with local authorities for internal use to inform their COVID-19 planning and response activity only.

Further information on local public comms to be confirmed.

Domestic abuse disclosures

Guidance produced by the City of London Police was issued on 1 May 2020. See Annex B.

Protective Security considerations

Guidance produced by Metropolitan Police Service Protective Security Operations was issued on 1 May 2020. See Annex A.

Risk assessment including Personal Protective Equipment for local authority staff

To follow.



Annex A: Protective Security Guidance for COVID-19 Testing Sites

GUIDANCE FOR COVID-19 TESTING SITES

One impact of the COVID-19 pandemic is that traditional crowded places, which are attractive terrorist targets, are now devoid of people. In light of the Government's lockdown and subsequent closure of large crowded places, COVID-19 Testing Sites could be seen as attractive venues to those intent on conducting terrorist activity.

The threat to the UK from terrorism remains at SUBSTANTIAL which means an attack is likely.

Current thinking suggests that an attack on a testing centre is possible but unlikely. However, the reduction in the number and frequency of crowds at other locations, and increased public focus on the health sector, could prompt some terrorists to consider healthcare facilities to be viable potential attack targets.

Some Testing Sites will have visible MOD support (personnel in military uniform) which may increase their attractiveness as a terrorist target. Testing Sites with queues of vehicles and staff testing may be vulnerable to attacks such as; Vehicle as a Weapon (**VAW**), Vehicle Borne IED (**VBIED**) and Marauding Terrorist Attack (**MTA**).

This guidance has been developed to support the establishment and operation of COVID-19 Testing Sites.

Due to the variety of different locations and operating processes being adopted, not all of the elements below will be applicable to all sites.

Security measures on site should seek to achieve the following:

- Deter hostile actors from targeting the Testing Site.
- Deter and identify hostile reconnaissance of the site.
- Restrict access of unauthorised people and vehicles to the site.
- Detect and delay any attempted attack before it reaches critical assets.



- Verify security alarm activations, at the perimeter and critical assets, and respond in a timely manner.
- Observe, with CCTV surveillance if possible, the entire critical asset and approach area.
- Relay ongoing situational awareness, to Police and emergency responders, during a security incident.
- Interrogate CCTV images (if applicable) and security alarm information during and post security incident.
- Monitor, respond and manage security alarms, and incidents, with dedicated security staff.
- Do not hinder the intended functioning of the venue.
- Give staff and visitors/participants a sense of security while not appearing intimidating or oppressive.
- Implement heightened security measures as part of your response to an increase in security threat.

When developing security solutions and plans for the Testing Site the following factors should be taken into account:

- Anticipated volume and arrival pattern of those attending.
- How many and what type of vehicles will need to be processed at the venue and at what times.
- The impact of any temporary overlay on the operation of an existing security system e.g. will a temporary building block the field of view of one or more existing CCTV units.



VEHICLE AS A WEAPON AND VEHICLE BORNE IED (VAW, VBIED)

Vehicles can be used in a variety of attack types including, ramming to clear a path for other potential attack methods, as a weapon in itself and as a delivery mechanism for a large explosive device.

Tactical options may include:

- Use of perimeter fencing to deter a vehicle attack against vehicles waiting for testing and staff employed on site – this can be Heras / SteelShield / Fortress fencing (or similar) depending upon the threat.
- Consider parking staff vehicles in a configuration around the Testing Site to provide a limited physical barrier to the rest of the site from hostile vehicles.
- If there are linear approaches to entrance points and staff locations, consider the positioning of vehicles, planters, barriers etc. to shield the staff (while still allowing for evacuation and rapid escape routes in the event of an incident). This could be as simple as a row of temporary signs – ‘something is better than nothing’.
- If possible chicane the queues of vehicles to reduce the opportunity for a hostile vehicle to accelerate.
- Temporary structures (marquees/large tents) should not be positioned to form part of the perimeter fencing – i.e. part of a tent requires “back of house” vehicle entry, therefore it is vulnerable to a parked Vehicle Borne Improvised Explosive Device (VBIED) or penetrative vehicle attack allowing entry into the Testing Site. Temporary structures should be situated within the perimeter or in a position to reduce the angle and approach speed of a vehicle.
- Staff should be directed not to congregate in crowds outside the Testing Site especially where moving vehicles can traverse to these locations with ease.
- The provision of training and guidance for security staff making it 100% clear as to what is expected of them and what they should do for all liveried, familiar or official vehicles such as emergency services vehicles in particular (these should not be waved through by security without verification of access passes).
- Be vigilant during large deliveries where access control may be weakened and exploited by criminals. Encourage areas of business involved in deliveries to obtain information about expected delivery time, driver and vehicles. Be mindful of persons or vehicles trying to tailgate.



MARAUDING TERRORIST ATTACK (MTA)

- **Reinforce Run Hide Tell message:** Be mindful given the current situation that the best advice is to disperse where possible rather than hide:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/595437/RHT_A5.pdf
- In the event of an Acid Attack a plentiful supply of water and appropriate PPE should be available.

PLACED IMPROVISED EXPLOSIVE DEVICE (IED) / PERSON BORNE IMPROVISED EXPLOSIVE DEVICE (PBIED)

In addition to a VAW or MTA style of attack the Testing Site could be vulnerable to an improvised explosive device (IED). Consideration should be given to the following;

- Protecting hazardous materials e.g. portable gas bottles. Areas storing hazardous materials should be protected to reduce the risk of unauthorised access. This should commence once the materials have been delivered on site and covered by 24hr shift coverage.
- Regular site checks by on site staff for anything out of the ordinary (Good Housekeeping) will remove the opportunity for suspicious items i.e. IED to be placed undetected and help maintain the Testing Sites operational effectiveness.
- Establish how far cordons would extend from the site in the event of an incident and consider the possibility of secondary devices at their evacuation muster points. Consider pre-planned concentric circles for key areas to denote 100, 200 400 metres etc.

SECURITY STAFF

At temporary sites established in response to COVID-19, it is important to reduce vulnerability, maintain a strong security culture and be prepared for (and resilient to) the threat and risk from terrorists. Please note this is not an exhaustive list of measures.

- Ensure critical assets such as generators are included within the patrol strategy.
- Ensure locations where test kits are stored overnight are included within a patrol strategy and monitored by CCTV if available.
- Complete ACT e-learning: An interactive online product designed to provide nationally accredited counter terrorism awareness to all. (45 minutes)
<https://www.gov.uk/government/news/act-awareness-elearning>



- Download NaCTSO ACT App: Live-time information from Counter terrorism (CT) Policing, plus all the latest protective security advice: <https://www.gov.uk/government/news/new-act-app-launched>.
- Distribute new CT Policing Z – Card: An aide memoire that gives advice and guidance on ‘Run, Hide, Tell’, actions for suspicious items, hostile reconnaissance, HOT principle, cordons, reporting incidents, CBRN and decision making:



20191017 NaCTSO Z
Card.pdf

- Onsite security and management to have clear points of contact with the local police and know how to report suspicious activity.

CCTV & LIGHTING

Depending upon the location chosen for the Testing Site there may be existing CCTV and lighting already in situ. The number of staff/participants and operating hours of the Testing Site may warrant temporary CCTV/Lighting being installed.

- CCTV should be monitored where installed.

COMMUNICATION

- Ensure that there are contingency plans in place for a communications failure so that communication does not break down between the command and control function and staff employed around the site.
- Advise all staff of their social media presence and not to share information relating to the site.



OTHER CONSIDERATIONS

Depending on the site location consideration should be given to involving neighbouring businesses or properties in the site emergency planning processes (this may already be in place where Testing Sites are established utilising locations that have a pre-existing security arrangements).

Utilise the 'Sixty Second Security Check List'. This is a quick list of security minded questions that all site staff should know the answers to in order to improve reactions to emergency situations:

- Who is appointed to make decisions at the site, and are they sure of their role?
- How do you enter and exit the site in an emergency?
- How do you lock down quickly? (If applicable)
- Where can you hide?
- How do you communicate/stay updated if you find yourself in a Run, Hide Tell scenario?
- Have you briefed this to your staff?
- Does everyone know the plan?
- Identify a suitable rendezvous point (RVP) for emergency response - this should be tested to establish its suitability.
- Identify contingencies if threat level increases e.g. security search regime / requesting permanent policing presence / daily defensive search of site / Hostile vehicle mitigation / closure of the site.

SECURITY ENHANCEMENT OPTIONS FOR AN INCREASE IN NATIONAL THREAT

Terrorism threat levels are designed to give a broad indication of the likelihood of a terrorist attack. They are based on the assessment of a range of factors including current intelligence, recent events and what is known about terrorist intentions and capabilities. The threat assessment is generic and does not identify any sector or specific location. As a result it is recommended that following the change in threat level those responsible for security review their plans and operations to provide a proportionate response.

All response plans should be prepared in advance, including a move to critical plan, so that options can be considered and established making implementation more efficient when required.



Further advice and guidance is available at;

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/616572/Threat Levels advice.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/616572/Threat_Levels_advice.pdf)

For further advice or information, please contact your local Police Counter Terrorism Security Adviser (CTSA) or Police Security Coordinator (SecCo).

OFFICIAL

Annex B: Dealing with domestic abuse disclosures

Domestic abuse is sometimes also called domestic violence and can involve a wide range of behaviour including violence, sexual abuse, threats, verbal abuse, emotional manipulation, controlling the victim and may involve harassing and stalking behaviour.

The victim may be reluctant to speak with an authority due to ongoing fear, control or manipulation. They may have little opportunity to seek help due to social distancing so could have been living with abuse for some time.

Things to do

Be sympathetic, use supportive language and be patient

Reassure them that they have done the right thing and you will help

Find a private space for them to speak

Are they or another person in danger now? If yes call 999.

Are they injured, sick or ill? Seek medical help.

Is the victim willing to speak with police? Encourage them to do so.

If you have trouble communicating, find someone to help. Consider language, gender, ethnicity etc.

Suggest they download the Bright Sky App (free) it's a covert app that looks like a weather app however it has details for support services in the local area and advice. It also has a quick link to call 999 if in danger

Things not to do

Don't question them in depth

Don't leave them alone, if they are talking to you, get someone else to assist you

Don't get them to repeat their story for other people or supervisors

Do not comment on what they could or should have done

Do not confront the suspect



<https://www.hestia.org/brightsky>

For women and children.
Against domestic violence.

<https://www.refuge.org.uk/>

Freephone 24-Hour National Domestic Abuse Helpline: **0808 2000 247**



<https://www.ncdv.org.uk/>

Call: 0800 970 2070 Text: NCDV to 60777 Email: office@ncdv.org.uk