

## **Prohibited and Controlled Articles**

### **Prohibited Articles**

Prohibited Articles are NOT PERMITTED on DOE-controlled property and are NOT ALLOWED to be stored in personally owned or government owned vehicles while those vehicles are on the site. Prohibited articles include items such as explosives; dangerous weapons, instruments, or material likely to produce substantial injury to persons or damage to persons or property; controlled substances (e.g., illegal drugs and associated paraphernalia but not prescription medicine if the person to whom it is prescribed is in possession of it); and other items prohibited by law.

While there are items that can be used as "dangerous weapons" (e.g., baseball bats, golf clubs), their primary purpose is not for harm or injury. Thus, these items are controlled and must remain stored in personally owned vehicles.

**This restriction includes but is not limited to the following:**

- Items prohibited by local, state, or federal law
- Privately owned explosive chemicals or devices
- Privately owned firearms of any kind including air-powered weapons
- Privately owned knives with blades that are 2.5 inches or longer
- Privately owned ammunitions/projectiles (e.g. bullets, rockets, arrows, etc., that could be discharged from a weapon)
- Illegal drugs and drug paraphernalia
- Items that can be used to start fires, excluding personal lighters (Note: Over-the-road and heavy-equipment truck drivers or personal vehicles are allowed to possess no more than five road flares as part of a vehicle's emergency inventory.)

### **Controlled Articles**

Controlled articles are items that are allowed on DOE-controlled property but are restricted from use in specified security areas. With the exception of key fobs and government-issued one-way pagers, electronic devices are prohibited in technical surveillance countermeasures (TSCM) areas without prior approval from the Officially Designated Federal Security Authority (ODFSA). These areas include classified conference rooms; Special Access Program areas; and areas where Top Secret information, weapons information with associated test data, or Sigma information is processed, produced, or discussed.

Government-owned electronic articles (e.g., wireless keyboards, a wireless mouse, mobile devices) must be evaluated and approved through the technical review process. Once a device is approved, employees who will use the device must sign a user agreement that outlines the restrictions and locations under which the device has been approved for use. If a device needs to be used in other areas of the site that were not approved under the original technical review process evaluation and signed user agreement, the device must be reevaluated before it is used.

Non-United States Government (USG) devices may not be connected to CNS systems or equipment without first being evaluated and approved. Devices must be submitted for approval through the CNS Technical Review Process (TRR) via Service Now. The only exception is that non-USG managed devices may connect to the visitor networks at Y-12 without an approved TRR. Employees, escorts, hosts, and subcontract technical representatives must ensure that visitors, vendors, and subcontractors are aware of device connection restrictions.

**Controlled articles include but are not limited to:**

- Hand-carried gas cans are approved safety containers for fuel, but only one 5-gallon tank per personal vehicle is allowed on-site. The gas can must also remain with the vehicle. The use of authorized gas cylinders must follow site-specific procedures.
- Portable Wi-Fi hot spots -Privately owned electronic devices (i.e., personal hot spots) with Wi-Fi hot-spot capability must remain in the PPA in a personally owned vehicle and must be disabled when possible. Hot-spot capability must be disabled on smartphones.
- Bluetooth may only be enabled on personal mobile devices and other personally owned devices outside in facility parking lots designated as GAAs/PPAs and while driving on access roads leading to or from GAA/PPA parking lots.
- Personal vehicles with video and/or audio recording capabilities (i.e., security equipment, Tesla Sentry Mode) must have features disabled while in the PPA.
- Personally owned removable storage devices (e.g., thumb drives, hard drives) must remain in a personal vehicle.
- Chemical irritants (e.g., pepper spray, mace) must remain in a personal vehicle.
- Use of lighters or other flame-producing devices must conform to site-specific safety procedures.
- At Pantex, key fobs are allowed except in nuclear explosive areas.
- Personal cameras or video equipment may be used at Y-12 cemeteries while under escort.
- Individuals are authorized to have a camera (digital, film, or video) or other camera equipment in the GAA (public area) of New Hope Center at Y-12. Individuals must ensure pictures are not taken of badges or individuals wearing badges while inside the GAA or visitor access control area.
- Photography inside New Hope Center at Y-12 is authorized only in the GAA (public area); only official, government-approved cameras with camera passes are allowed in the access-controlled office area of New Hope Center. Photography outside New Hope Center is not authorized.
- At Pantex, photography in the GAA is not authorized unless otherwise posted by signage. If or when pictures are taken, individuals must remove badges (Homeland Security Presidential Directive-12 and/or local site-specific only) and hide them from view of the camera.

**Secure Spaces (Limited Area, Protected Area, Material Access Area)**

The introduction and use of any mobile devices (either managed or not managed by the U.S. government) in CNS LAs, PAs, and MAAs is prohibited except for the following:

- NNSA-approved, USG mobile devices for use by designated emergency response personnel as an element of their daily job responsibilities
- Devices approved on a case-by-case basis by the ODFSA
  - When the ODFSA approves the use of mobile devices, all camera functions on those devices must be disabled and all microphone functions must be restricted to only the native telephone application while in secure spaces. Exceptions to this requirement may only be approved by the NNSA Chief of Defense Nuclear Security and must be supported by

a critical mission need.

- Approved mobile devices that have traveled outside the United States or into foreign embassies and consulates may be reintroduced in secure spaces only after cyber security and TSCM evaluations have ruled out the possibility of compromise.
- At Pantex, use of USG mobile devices during emergency response is not authorized inside MAA facilities (i.e., bays, cells, igloos, ramps, or buildings).

## **Vehicle Security**

When left unattended at onsite and at offsite locations, government and other business use vehicles (e.g., vendor, subcontractor, Tiger Truck, Polaris Ranger, Kubota side-by-side, etc.) and construction and boom lift equipment (e.g., bucket trucks, transportable cranes, snorkel-lifts, etc.) must be locked with the keys/fob removed.