Request and Consent to Secure Electronic Device

Communitas
Empowering people. Enriching lives.

Date effective: 2/26/14
Revisions: 4/2/14, 3/25/16, 3/19/18
Review date: 9/19/22
HRC Review: 12/7/22

Applies to: all

Policy number: 6.0.27
Regulatory reference: 115 CMR 5.10 (1)

S:\Agency Policy\6 - Program Related Policies and Procedures\6.0.27 Request and Consent to Secure Electronic Device Policy

---

- An individual may request that employees secure electronic devices in a locked location when not in use. If a request has been made to secure an electronic device while not in use, the form Request and Consent to Secure Electronic Device must be completed and kept in the person's legal file. This form must be completed annually.
- Items are only to be secured at the request of the person owning the item. Securing of items cannot be done as punishment or in retaliation.
- If an electronic device is withheld from an individual and secured as part of an approved Behavior Plan that has been reviewed by the Human Rights Committee, the Behavior Plan must have the consent of the individual, and guardian if the person has one.
- A Request and Consent to Secure Electronic Device does not transfer ownership of the device, and nothing in this policy or in any of the required forms should be construed to imply ownership of the secured device by Communitas or by any employee of Communitas.

Procedure:

1. Complete the form Request and Consent to Secure Electronic Device and obtain all needed signatures. Each section must be filled out completely.
2. Indicate on the form if the charger or any other accessory for the device is also going to be secured when not in use.
3. Any time the individual is not using the device, it will need to be locked in a secure location, in a locking cabinet or safe. The Medication Closet cannot be used for this purpose; it must be in a separate locked area.
4. Each time the individual requests the device, an employee must log it out, including date, time, employee's name and signature, on the Secured Device Log.
5. Each time the device is returned to an employee to be secured, it must be logged in, including date, time, employee's name and signature, on the Secured Device Log.
6. Periodic checks must be completed by the Program Director to ensure the log is being completed correctly, and that all electronic devices (and any accessories) are accounted for.

Associated forms:

S:\Blank Forms\Consent Forms\Request and Consent to Secure Electronic Device.docx
S:\Blank Forms\Secured Device Log.docx