

---

**Overview**

This standard is about following up electronic monitoring incidents in the field which includes responding to instructions from call centres, visiting premises, collecting information about incidents and, when necessary, repairing or replacing equipment.

Incidents could include unauthorised absences, equipment malfunction, equipment tampering, loss of electrical power, loss of the telephone connection, eviction from the premises, inability to enter the premises and entry into a proscribed area.

**There are three elements**

- 1 Assess incidents and prepare to take action
- 2 Deal with incidents
- 3 Carry out random alternative monitoring

**Performance**

**criteria**

**Assess incidents and prepare to take action**

- You must be able to:
- P1 obtain information about incidents in accordance with your organisation's procedures
  - P2 clarify uncertainties you have in accordance with your organisation's procedures
  - P3 check with supervisors what you should do when incidents occur in accordance with your organisation's procedures
  - P4 agree incident priorities in relation to your work schedule where required in accordance with your organisation's procedures
  - P5 verify you have necessary equipment and access to personnel in accordance with your organisation's procedures:
  - P6 check location of incidents in accordance with your organisation's procedures, and:
    - P6.1 identify plans of action
    - P6.2 follow best routes to location
    - P6.3 advise relevant people of your arrival
  - P7 carry out initial risk assessments of locations in accordance with your organisation's procedures including:
    - P7.1 what is known about individuals being monitored

**Deal with incidents**

- You must be able to:
- P8 introduce yourself to relevant people in accordance with your organisation's procedures, and:
    - P8.1 show proof of your identity
  - P9 check correct individuals are being monitored in accordance with your organisation's procedures
  - P10 evaluate further risks during incident-situation in accordance with your organisation's procedures
  - P11 take actions based on factors present at incidents in accordance with your organisation's procedures

- P12 obtain information from individuals being monitored about incidents in accordance with your organisation's procedures
- P13 obtain signed statements from individuals being monitored, where required, in accordance with your organisation's procedures
- P14 advise relevant people of actions taken in accordance with your organisation's procedures, and of:
  - P14.1 your departure from site
- P15 complete required records in accordance with your organisation's procedures

**Carry out random alternative monitoring**

- You must be able to:
- P16 establish random alternative monitoring is needed in accordance with your organisation's procedures
  - P17 obtain necessary information to proceed with random alternative monitoring in accordance with your organisation's procedures
  - P18 check you have equipment for random alternative monitoring in accordance with your organisation's procedures, and:
    - P18.1 equipment is functioning correctly
    - P18.2 configure equipment where required
  - P19 make sure you are within range of required sites to receive clear signals in accordance with your organisation's procedures
  - P20 report results as required in accordance with your organisation's procedures
  - P21 repeat random alternative monitoring within organisational timescales
  - P22 complete required records in accordance with your organisation's procedures

## SFJFG5

### Follow up electronic monitoring incidents in the field

---

#### Knowledge and understanding

- You need to know and understand:
- K1 your legal responsibilities for electronic monitoring
  - K2 different types of electronic monitoring
  - K3 organisational authorisation procedures
  - K4 common types of electronic monitoring incidents and how to respond to them
  - K5 essential pieces of information needed to assess incidents
  - K6 how to prioritise incidents in terms of work schedules
  - K7 how to select 'best' routes including using navigational aids
  - K8 how to carry out risk assessments of areas and make use of information you have been given about individuals being monitored
  - K9 how to carry out random alternative monitoring
  - K10 the equipment required to carry out random alternative monitoring
  - K11 how to ensure you are within adequate range for clear signals
  - K12 why it is important to identify individuals being monitored and how to do so
  - K13 the importance of introducing yourself and showing proof of identity
  - K14 how to question individuals about incidents
  - K15 how to test, maintain and replace electronic monitoring equipment
  - K16 manufacturer's instructions for equipment care
  - K17 how to correct problems with equipment when required
  - K18 where it is important to obtain signed statements from individuals being monitored
  - K19 organisational procedures for keeping records including reporting results of random alternative monitoring

**Additional Information**

**Glossary**

**Relevant people** can refer to individuals, others relevant or significant to individuals, staff in your own agency including investigating teams or staff from other agencies.

**Organisational procedures** can include prison service instructions, prison policies, legislative policies and any other policies and procedures used across custodial care in the UK.

## SFJFG5

### Follow up electronic monitoring incidents in the field

---

**Developed by** Skills for Justice

---

**Version number** 2

---

**Date approved** October 2013

---

**Indicative review date** October 2018

---

**Validity** Current

---

**Status** Original

---

**Originating organisation** Skills for Justice

---

**Original URN** SFJ FG5

---

**Relevant occupations** Prison staff; Prison manager; Governor; Officers; Public Service Professionals; Youth Justice Officers; Youth Offending Team Officers

---

**Suite** Custodial Care

---

**Key words** Respond; electronic; monitoring; equipment; tagging; individuals; incidents; breaches; random; checks; alternative; risks; statements