STANDARD OPERATING PROCEDURE
FORENSIC - ELECTRONIC EQUIPMENT FOR USE BY STAFF, VISITING PROFESSIONALS AND CONTRACTORS

Document Reference	SOP20-020
Version Number	1.2
Author/Lead **Job Title**	Thomas Greenwood Health, Safety, and Security Lead.
Instigated by: **Date Instigated:**	Security Committee September 2020
Date Last Reviewed:	13 March 2023
Date of Next Review:	March 2026
Consultation:	Paula Phillips, Director of secure services Pattie Boden, Clinical Director of secure services Helen Courtney, Modern Matron Richard Weldrick, Modern Matron Security Committee
Ratified and Quality Checked by: **Date Ratified:**	Director sign-off (Paula Phillips) 13 March 2023
Name of Trust Strategy / Policy / Guidelines this SOP refers to:	

VALIDITY – All local SOPS should be accessed via the Trust intranet

CHANGE RECORD

Version	Date	Change details
1.0	*Sept-20*	*New SOP.*
1.1	*Nov-21*	*Reviewed.*
1.2	*Mar 2023*	*Reviewed and approved by director sign-off (Paula Phillips – 13/03/23).*

Contents

1. INTRODUCTION

It is increasingly difficult for staff working in health services to work without the use of IT equipment. This same equipment may, if misused, compromise the security of low and medium secure services.

The Humber Centre and Pineview are using of electronic records, and this will require the use of PCs, laptops and tablet devices.

This procedure is intended to support the use of certain items of electronic equipment within the secure perimeters of the Humber Centre, Pineview and South West Lodge, namely;

- Still and video cameras,
- Tablet devices,
- Laptop computers (including netbooks, etc.)
- Mobile Telephones (in exceptional circumstances as agreed with the security team)
- Some electronic tools that may have a very specific purpose in certain repair, maintenance, recording or monitoring tasks

(For the remainder of this procedure described as 'electronic equipment')

2. SCOPE

This procedure is aimed at all staff working in the service, and at any visiting trust staff or contractors who may have need of electronic equipment to fulfil their role. This also includes professional visitors (e.g. outside doctors undertaking assessments, solicitors etc.).

3. PROCEDURE STATEMENT

All staff who, under this policy are permitted to bring electronic equipment into the Humber Centre and Pineview (including South West Lodge), will do so in accordance with their duties and responsibilities to adhere to Information Governance and Confidentiality policies.

4. DUTIES AND RESPONSIBILITIES

All staff will be aware of this procedure and will work in accordance with it.

5. PROCEDURE

5.1. PHILOSOPHY

The service's approach is that only devices which are explicitly detailed in this protocol can be brought into the building. Any devices not listed cannot be brought into the building.

5.2. USE / ACCESS

The following portable electronic / media devices may be brought into the Humber Centre and Pineview, under the controls as described;

MP3 Players / iPods

- Staff only (for personal use, e.g. travelling to and from work).
- Only models with no voice or video recording, and without .communication capability.
- Not for use in clinical areas.

Laptop Computers / tablets (includes iPad)

- To be stored in non-clinical areas.

- Escorting staff will monitor appropriate use.

Mobile Telephones

- Mobile Phone can be accessed upstairs in the Humber Centre. They must be brought into the unit via the staff airlock and straight upstairs, via the upstairs access point.
- Specialist Community mental health team (SCFT) may take trust issued mobile phones through the building for use in the SCFT offices in the annex at Pine View.
- No personal mobile to be carried or used in any other area within the secure perimeter other than upstairs at the Humber Centre.
- Staff are not to use cameras on mobile phones whilst within the secure perimeter. Any use of a camera within the secure perimeter would be consider gross misconduct and will be managed through the disciplinary process.
- Permissions to be granted for use any other area only in circumstances that are necessary for completion of estates works only, this may include use of a camera, but this must be agreed and planned. Authorisation must be sought from the security team and a permissions form completed. (Appendix 1)

Cameras – still & video

- Any images of aspects of the building must be absolutely necessary to the task in hand, and may be limited for security reasons

PDA Devices

- For use by Trust staff or contractors for whom the equipment is essential in order to undertake required tasks.
- Escorting staff will monitor appropriate use.

Emergency Services Equipment

- Any equipment required by the emergency services (police, fire, ambulance) can be brought in. Escorting staff will ensure that they monitor use as far as is reasonably possible.

5.3. EQUIPMENT FOR ROUTINE USE IN CLINICAL AREAS

- Each Ward Security Profile (WSP) will describe the risks attached to the use of electronic equipment and the relevant control measures in place.

5.4. STAFF WITH ACCESS TO SECURITY EQUIPMENT

- Staff will routinely be expected to use electronic equipment that is supplied explicitly for use in service buildings – this will include desktop PCs, laptops and tablet devices.
- Staff will discuss the need to bring in any additional electronic equipment with their line manager and / or Security Lead, and If the need is supported, the form in appendix ‘A’ is completed and;
- Copy to staff member
- Copy to personal file
- Copy to the Security Lead (to be stored in reception, attached to that staff member’s original security induction)

5.5. OTHER TRUST STAFF

- Staff will discuss the need to bring in electronic equipment with the Security Lead (or member of the Senior Management Team if unavailable)
- If the need is supported, the form in appendix ‘A’ is completed and;
- Copy to staff member
- Copy to personal file via their line manager
- Copy to the Security Lead (to be stored in reception)

5.6. VISITING PROFESSIONALS / CONTRACTORS

- Any request made by a visiting professional / contractor will, ideally, be made in advance. However, it may be that this is not possible , and an ‘on-the-day’ decision may be required

- Where possible, the consideration will be made by the Security Lead or member of the Senior management Team or Ward Manager / Charge Nurse
- If the need is supported, the form in appendix 'A' is completed and;
- Copy to visiting professional / contractor
- Copy to the Security Lead (to be stored in reception)

5.7. RECEPTION CONTROL ROOM STAFF

- A paper copy of each authorisation form will be maintained in the reception control room, which be used by reception staff to ensure that any electronic equipment that is being brought in is approved by this process.
- Reception staff will not negotiate around this issue, and any dispute / lack of clarity will be referred to the Security Lead wherever possible, otherwise to a Ward Manager / Charge Nurse or co-ordinator.
- Reception staff will log all electronic devise coming into the secure perimeter. (appendix 2)

5.8. BREACH

In the event of an individual breaching this protocol, the following guidance is offered;

5.8.1 Staff

1. Remedial action, with utmost consideration for maintaining safety and security followed by Datix – copy to Security Lead
2. Fact finding / adverse incident investigation
3. HR advice gained regarding individual accountability / capability
4. Appropriate action under Trust's Disciplinary Policy

5.8.2 Visitors (official, visiting professionals, other Trust staff, etc.)

1. Immediately remove / make safe contraband item(s),
2. Discuss with visitor, raise awareness,
3. Consider requesting the visitor to cease the visit,
4. Complete Datix – copy to Security Lead who will liaise with visitor / team / company / manager as appropriate.

5.8.3 Contractors

1. Immediately remove / make safe contraband item(s),
2. Discuss with contractor, raise awareness,
3. Consider (safely) ceasing the work in progress if necessary (consult with senior staff as are available),
4. Complete Adverse Incident form – copy to Security Lead who will liaise with facilities Dept.

6. IMPLEMENTATION

All new staff will be required to read the service procedures as part of their service security induction and security refresher.

7. MONITORING AND AUDIT

This procedure will be monitored by the Security Committee.

8. REFERENCES/EVIDENCE/GLOSSARY/DEFINITIONS

Nil to reference

APPENDIX 1 - FORENSIC MENTAL HEALTH & LEARNING DISABILITIES SERVICE USE OF PROHIBITED IT / ELECTRONIC EQUIPMENT WITHIN THE SECURE PERIMETER CONTRACT

Name	
Position	
Organisation	
Item(s) to be used	
Reason it is necessary to bring the item(s) into the building	
'One off' request or ongoing (give details)	

I have discussed the use of this item within the secure perimeter of the Humber Centre and Pineview (including South West Lodge), and have explained the need to bring it into the building,

I understand that this item is prohibited, and that to use it is an exception to usual practice,

I understand that the item could, if used inappropriately, jeopardise some or all of the following;
Safety / security of staff and / or patients,
Confidentiality / right to privacy of staff and / or patients,
The integrity of my property, and any information stored thereon,
and I undertake not to use it in such a way as might compromise any of the above

I confirm that the device is password protected and encrypted

I understand that the device must be kept in my possession at all times and must not be used by any patient unless it has explicitly been brought in for that purpose (e.g. patient satisfaction surveys, etc.)

I understand that if any member of staff has reason to suspect that it is being used out with the agreed parameters it will be confiscated until I leave the premises

Details of discussion;

Details of any control measures;

Signed staff;

Request Supported by (name & signature);

Date;

APPENDIX 2 - FORENSIC MENTAL HEALTH & LEARNING DISABILITIES SERVICE PORTABLE ELECTRONIC MEDIA DEVICE TRACKING FORM

Name	
Date [of visit]	
Organisation	
Details of device(s) being brought into the building	

I have read the Non-patient access to portable electronic media devices procedure.

I understand that the above item is controlled under the security strategies in place at the Humber Centre / Pine View, [and that I may be guided in its use by escorting staff] (delete for security inducted staff).

The device that I am bringing into the building does / does not have communication capability. [I am aware of the significance of this, and that I must utilise that capability, whilst within the secure perimeter, in a way that does not compromise the safety, privacy and dignity of patients and staff] (delete if not appropriate)

Signed:…….. (Visitor / contractor / staff member)

Signed:…….. (Staff)

Date: