1. Introduction:

This procedure aims to provide clear guidance for the use of mobile phones and/or Electronic recording equipment for service users within ███████ in-patient and out-patient/day service areas.

It aims to set out clear guidance as to when the use of such equipment can be Considered to be unreasonable.

This procedure aims to strike a balance between the confidentiality and right to privacy of individuals and the need to protect vulnerable adults, maintaining their health and safety in terms of safeguarding them from potential abuse.

Furthermore, as mobile phones have photographic and audio recording capability, it is the assumption that they could be used for this purpose and therefore have the potential to grossly infringe upon the privacy of others.

Staff should make every effort to support patients in making and maintaining contact with their family and friends by telephone (either personal mobile or using the phones available on the wards). This contact should be recognised as an essential element of support and comfort.

This procedure has been developed in accordance with the following documents:
Using Mobile Phones in NHS Hospital, (Department of Health, May 2007)
Code of Practice to the Mental Health Act 1983 (Department of Health, 2008).

The guidance within this procedure may also be applied where the mobile phone is being used for any other purpose including gaming, web access or mobile television.

This procedure applies to all people who use services, both as inpatients and those attending out-patient services that need to maintain their social networks and visitors to Trusts` premises.

Highlighted areas of this procedure specifically cover inpatients who are detained under the Mental Health Act 1983 and their access to mobile phones.

Decisions under the Act must be taken with a view to minimising the undesirable effects of mental disorder, by maximising the safety and wellbeing (Mental and physical) of patients, promoting their recovery and protecting other people from harm.

2. Definitions:

• Mobile Phone
A mobile phone for the purpose of this policy is any mobile communications device, phone, PDA or other equipment which may be used to record others or transmit conversation.

• Least Restriction:
People taking action without a patient's consent must attempt to keep to a minimum the restrictions they impose on the patient's liberty, having regard to the purpose for which the restrictions are imposed.

• Respect:
People taking decisions under the Act must recognise and respect the diverse needs, values and circumstances of each patient, including their race, religion, culture, gender, age, sexual orientation and any disability. They must consider the patient's views, wishes and feelings (whether expressed at the time or in advance), as far as they are reasonably ascertainable, and follow those wishes wherever practicable and consistent with the purpose of the decision. There must be no unlawful discrimination.

• Participation:
Patients must be given the opportunity to be involved, as far as is practicable in the circumstances, in planning, developing and reviewing their own treatment and care to help ensure that it is delivered in a way that is as appropriate and effective for them as possible. The involvement of carers, family members and other people who have an interest in the patient's welfare should be encouraged (unless there are particular reasons to the contrary) and their views taken seriously.

• Effectiveness, efficiency and equity:
People taking decisions under the Act must seek to use the resources available to them and to patients in the most effective, efficient and equitable way, to meet the needs of patients and achieve the purpose for which the decision was taken Throughout the policy document we have tried to highlight where a particular principle can be applied specifically but staff **must** apply the principles to all decisions. Any decision to depart from the directions of the policy and the Code of Practice must be justified and documented accordingly in the patient's case notes. Staff should be aware that there is a statutory duty for these reasons to be cogent and appropriate in individual circumstances.

3. Mobile Phone Procedures:
3.1. Procedure for Out Patient Clinics:
Staff should discourage patients and visitors from bringing their mobile phones onto day care units and into out-patient clinics.
Staff should inform patients of the risk of theft/loss of the mobile phone and the restrictions placed on the use of mobile phones. Those who choose to retain their mobile phones must be informed of and asked to consent to the following Restrictions placed on their use:

• No use of the recording or photography facility

• To have equipment on a silent setting
• Not to use equipment during therapeutic activities
• Not to lend equipment to other patients
• Not to use in communal areas
• Charging of mobile phones is to be limited to a designated area.

3.2. Procedure for Inpatient Units:

Discourage patients and visitors from bringing their mobile phones onto Inpatient units due to the potential of theft and loss.

Inform patients of the risk of theft/loss of the phone and the restrictions placed on the use of mobile phones. Those who choose to retain their mobile phones must be informed of and asked to consent to the following restrictions placed on their use:

• No use of the recording or photography facility
• To have equipment on a silent setting
• Not to use equipment during therapeutic activities
• Not to lend equipment to other patients
• Not to use in communal areas.

This may need to be repeated for patients who have fluctuating capacity. For other patients and visitors they may need to be informed at the point of admission or on their first visit. The terms of this policy should be displayed in the ward area to prevent the necessity for repeating this information on a regular basis.

Permission is to be requested by the patient who wishes to use a charger to the mobile phones. In deciding whether or not to grant permission, the clinical team must undertake an appropriate risk assessment. Charging of mobile phones is to be limited to a designated area as decided by the Ward Manager or Inpatient Services Manager.

A full and comprehensive risk assessment needs to take place in respect to the inpatient who has access to a mobile phone and particular the charger for 2 reasons: -
• The equipment will not be PAT tested, and
• The charger could be used as a potential ligature

All in patient units should have a designated public telephone, which is sited in an area that promotes and protects privacy as far as reasonable practicable. Installation of booths or hoods is considered to be best practice for wards.

Conversations should be treated as confidential involving sensitive patient information. There is therefore a need to maintain the balance between

competing needs of:

• Protecting confidentiality of the caller and others
• Protecting vulnerable individuals from abuse
• Protecting the rights of individuals
• Providing a therapeutic environment, and
• Maintaining people who use services, that they continue contact with
Social networks.

The following guide has been agreed in conjunction with young people and ward based staff:

- Phone calls to be made in quiet room/bedroom.
- Mobile phones to be kept on a patient's person or stored in the ward office when not in use.
- Phones to be handed into the nursing office at midnight for charging and to promote sleep hygiene.
- Phones are to be labelled for easy identification.
- Patients advised not to take pictures of staff, clinical areas and/or clinical information.

If there are concerns in regards to the misuse of mobile phones, the nursing staff will care plan phone use for individual patients which may include:

- Supervised use.
- Limited use.
- Use of phone for music only.

In the event that a media device is removed from any patient this must only be done so when absolutely necessary and only where there is a risk to self or others which cannot be managed in a less restrictive way. All devices must be stored safely until they can be returned at the earliest opportunity to the service user or their nearest relative. All property must be signed in and signed out and staff made aware of this procedure, the trust takes no responsibility for any digital media with photographic capabilities

Social media:

Patients are asked to not contact staff through social media. Staff are encouraged to report such incidents through the Trusts' DATIX incident reporting procedures.

Patients are also asked to not write about their hospital admission or identify peers online.

Staff have been advised to monitor security settings if they use social media to further protect against such incidents occurring.

Safeguarding concerns:

There is a need to ensure that young people are aware of the need for support and guidance around safe internet usage. Appendix one highlights 10 ways in which young people can stay safe online. It is the responsibility of each key nurse to explore internet safety issues with patients on admission.

Breach of Guidance Principles:

Service users found to be in breach of the restrictions laid out in this guidance may have their equipment confiscated and placed in storage or sent home with parents / carers until a clinical review of the breach has taken place.

- The Patient Property protocol must be followed if the service user equipment is removed to ensure there is a record of the phone being held.
- Any recordings by equipment contrary to this guidance should be instantly deleted and an incident form must be completed detailing all breaches contained in this guidance.
- An entry of all breaches should be recorded in the appropriate case notes relating to the service user concerned.

Appendix 1: Breach Guidance Principles

Name	Verbal Warning	Written Warning	Removal Of Phone
	Date of Warning: Datix ID: Staff Name: Brief Details of Breach:	Date of Warning: Datix ID: Staff Name: Brief Details of Breach: Letter Completed by: Date Letter Sent:	Date Phone Removed: Datix ID: Staff Name: Brief Details of Breach: Where Item is being Stored (unit / home): Review Date:
	Date of Warning: Datix ID: Staff Name: Brief Details of Breach:	Date of Warning: Datix ID: Staff Name: Brief Details of Breach: Letter Completed by: Date Letter Sent:	Date Phone Removed: Datix ID: Staff Name: Brief Details of Breach: Where Item is being Stored (unit / home): Review Date:
	Date of Warning: Datix ID: Staff Name: Brief Details of Breach:	Date of Warning: Datix ID: Staff Name: Brief Details of Breach: Letter Completed by: Date Letter Sent:	Date Phone Removed: Datix ID: Staff Name: Brief Details of Breach: Where Item is being Stored (unit / home): Review Date:
	Date of Warning: Datix ID: Staff Name: Brief Details of Breach:	Date of Warning: Datix ID: Staff Name: Brief Details of Breach: Letter Completed by: Date Letter Sent:	Date Phone Removed: Datix ID: Staff Name: Brief Details of Breach: Where Item is being Stored (unit / home): Review Date:

Appendix 2: 10 Steps to internet safety.

Staying Safe Online

1)   Don't post any personal information online – like your address, email address or mobile number.

2)   Think carefully before posting pictures or videos of yourself. Once you've put a picture of yourself online most people can see it and may be able to download it, it's not just yours anymore.

3)   Keep your privacy settings as high as possible

4)   Never give out your passwords

5)   Don't befriend people you don't know

6)   Don't meet up with people you've met online. Speak to your parent or carer about people suggesting you do

7)   remember that not everyone online is who they say they are

8)   Think carefully about what you say before you post something online

9)   Respect other people's views, even if you don't agree with someone else's views doesn't mean you need to be rude

10) If you see something online that makes you feel uncomfortable, unsafe or worried: leave the website, turn off your computer if you want to and tell a trusted adult immediately.