

## Policies, Procedures, Guidelines and Protocols

Document Details		
Title		Internet access and use for Patients and Visitors – respecting privacy and confidentiality
Trust Ref No		1990-49132
Local Ref (optional)		
Main points the document covers		This document sets out the way in which we would ask patients and visitors at our sites to respect the privacy and confidentiality of other patients, visitors and staff when using the internet, and how we will respond to any issues that are reported.
Who is the document aimed at?		All staff, patients and visitors
Author		Chris Hudson, Head of Communications
Approval process		
Approved by (Committee/Director)		Information Management & Technology Strategy Group
Approval Date		04/03/2019
Initial Equality Impact Screening		Yes
Full Equality Impact Assessment		No
Lead Director		Director of Finance
Category		
Sub Category		
Review date		04/03/2022
Distribution		
Who the policy will be distributed to		All staff and made available to the public via the website
Method		Via team meetings and corporate induction and the policy will be available on the website. Posters will also be displayed in public areas.
Document Links		
Required by CQC		
Required by NHSLA		
Other		
Amendments History		
No	Date	Amendment
1	08/01/2019	Minor amendments made to staff names. Document to be noted at IM&T meeting in March 2019.
2		
3		
4		
5		

## Contents

1	Introduction .....	2
1.1	Definitions.....	3
2	Objectives .....	3
3	Duties.....	4
4	Use of computers and mobile phones .....	4
5	Wifi Access.....	5
6	Guidance for patients and visitors .....	6
7	Review arrangements .....	6
8	Associated documents .....	6
	Appendix 1 – Photography and Video Recording Guidance.....	7
	Appendix 2 – Respecting Privacy and Confidentiality.....	8

## 1 Introduction

We recognise that the use of electronic communications and the internet are widespread, and that many patients and visitors at our sites have access to their own electronic devices, such as mobile phones or tablets. It is important that all of these technologies are used sensibly and not in a way that infringes the privacy or confidentiality of others. This policy aims to ensure that patients and visitors are aware of the guidelines we have in place to protect the privacy of others, and that staff are also aware of the guidelines to help patients and visitors adhere to them.

This policy applies to accessing the internet, including email, which can be used for communicating information within the public domain. This includes social media websites (such as Facebook and Twitter) and any other public forums, online publications or blogs. This policy applies at all times on premises used or owned by the Trust.

What is Confidential Information?

Confidential information within the NHS is commonly thought of as health information; however, it can also include information that is private and not public knowledge or information that an individual (e.g. staff, patient or visitor) would not expect to be shared. It can take many forms including patient level health information, employee records, occupational health records, photographs and recordings etc. It also includes Trust confidential business or sensitive information.

What is the Data Protection Act (DPA)?

The Data Protection Act (DPA) (1998) applies to living individuals and gives those individuals a number of important rights to ensure that personal information covered by the Act is processed lawfully. It regulates the manner in which such information can be collected, used and stored, and so is of prime importance in the context of information sharing.

There are eight Data Protection Principles:

1. Personal information must be fairly and lawfully processed
2. Personal information must be processed for limited purposes
3. Personal information must be adequate, relevant and not excessive
4. Personal information must be accurate and up to date
5. Personal information must not be kept for longer than is necessary
6. Personal information must be processed in line with the data subjects' rights
7. Personal information must be secure
8. Personal information must not be transferred to other countries without adequate protection

The Human Rights Act (1988)

Human Rights issues have an influence in relation to data protection - Article 8 says that: "Everyone has the right to respect for his private and family life, his home and his correspondence".

## 1.1 Definitions

**Trust:** Shropshire Community Health NHS Trust.

**Our sites:** Premises owned or used by the Trust and its partners.

**Visitor:** This is anyone attending our sites that is not a patient or member of staff, for example someone visiting a patient, someone attending a site from a non-NHS organisation, such as a contractor, volunteer, or a VIP guest attending a formal or informal event.

**Staff:** This is anyone working directly for the NHS or its partners.

**Patient:** This is anyone being assessed or receiving health care provided by the NHS or its partners.

**Personal data:** is information that affects (a person's) privacy, whether in their personal or family life, business or professional capacity. Personal data is defined as any information relating to an identified or identifiable natural person, this includes photographs.

**Social Media:** Websites and applications that enable users to create and share content or to participate in social networking (such as Facebook, Instagram and Twitter etc...).

**Blogs:** Websites and services including chat rooms and forums where people share thoughts, opinions and ideas.

**Electronic device:** This includes computers, laptops, tablets, mobile phones, portable gaming systems, cameras etc...

## 2 Objectives and Scope

All NHS hospital trusts should have a robust policy setting out how access by patients and visitors to the internet and to social media activities such as blogs and Twitter is managed and where necessary restricted. Such a policy should be widely publicised to staff, patients and visitors and should be regularly reviewed and updated as necessary.

We are committed to protecting the privacy and dignity of our patients, and to support our staff at work. The purpose of this policy is to:

- Safeguard the privacy and confidentiality of our patients and visitors to our sites
- Help to ensure the safety and wellbeing of patients and visitors at our sites
- Safeguard the privacy and confidentiality of our staff
- Ensure confidential business or sensitive information is protected
- Help people understand how they can use the internet in accordance with our guidelines
- Make sure the Trust is not exposed to legal and governance risks from the use of electronic communications and the internet

This policy covers the use of both privately-owned and Trust-owned electronic devices accessing the internet and related services such as social media and email.

This policy applies to all patients and visitors on our sites.

The Trust cannot and will not guarantee the confidentiality or security of data over any public mobile network or wireless connection.

### 3 Duties

**Director of Finance** has Board level responsibility for development, maintenance and review of this document.

**All Senior Managers** are responsible for disseminating and implementing this policy.

**The Head of Communications** is responsible for the Trust's social media activity.

**All staff** are responsible for helping to ensure that the privacy and dignity of patients and their colleagues is protected. They are also responsible for bringing the guidelines to the attention of patients and visitors. Staff conduct when accessing these types of services is covered in the Trust's Information Security Policy.

### 4 Use of electronic devices at our sites

We understand that patients and visitors are likely to have access to electronic devices, which they can use to access the internet, social media, emails and blogs at our sites. When using these electronic devices we would ask that they do so respectfully of others and in accordance with the guidance set out in this policy.

Patients and visitors are reminded to consider the privacy of other patients, visitors and staff on our sites. Patients and visitors may overhear conversations or see certain information about other patients or members of staff. Therefore, we would ask patients and visitors to maintain the confidential and private nature of this information by not sharing these details without informed consent.

Confidentiality and privacy can also extend to talking and sharing photographs. Taking any photographs of patients, visitors or staff on our sites without informed consent is not permitted.

If taking a photograph or video at our sites please be mindful of other people's right of privacy, and for patients to be treated confidentially with dignity and respect. Please take time to think who is in the background or what is being discussed next to you.

If you are unsure about this policy or any related guidance please speak to a member of staff who will be happy to help (for example, if someone wanted to take a picture of a relative in hospital then a member of staff could advise how to do this without impeding anyone else's privacy, or could even take the picture for you).

The above also applies to other guests or visitors to our sites, such as VIPs. All photography and video recording should be carried out with the guidance of a member of staff and in accordance with this policy.

If evidence of and breach of confidentiality or privacy is discovered, or a patient or visitors is experiencing harassment, we may ask for the visitors to be removed, or patient to cease using their electronic device.

We may also choose to take further action if any inaccurate, misleading or defamatory information is posted over the internet about patients, visitors, the Trust or members of staff.

Media and websites capable of causing offence to others, for example, sexually explicit, indecent or illegal material, must not be accessed on our sites.

The display of any offensive material in a public area (audio or visual) is strictly prohibited.

The Trust reserves the right to restrict access to websites it deems inappropriate.

## **5 Trust Wifi Access**

Where wireless internet access is provided for patients and visitors by the Trust it is done so without warranty or support and is not classified as a secure means of access. Therefore, users accessing this wireless network do so at their own risk. The Trust is not responsible for the loss, misuse or theft of any information, passwords or other data transmitted by users.

The Trust does not provide any form of technical support for patients or their visitors.

Users must accept the terms and conditions set out in this policy in order to access and utilise the service.

The reproduction, upload or download of information (of which the user does not hold the copyright or responsibility) is illegal without permission from the copyright holder.

The display of offensive material in any publicly accessible area is strictly prohibited.

Using Wifi access to transmit any material (by email, uploading, posting, or otherwise) that, intentionally or unintentionally, violates any applicable law, or any rules or regulations promulgated there under is strictly prohibited.

It is forbidden to use any Trust Wifi connection for commercial gain by the user or a third party, for example you must not use the Trust Wifi for business use.

A user must not deliberately perform any act that will impair the operation of any electronic system or network. This includes the wilful or ignorant wasting of system or network resources by sending large volumes of spam, generating large volumes of printed output, or the wilful creation of heavy network traffic.

Any Devices which are network intrusive and could potentially interrupt network services, or change the Trust's Data Network topology in any way are prohibited. Prohibited devices include but are not limited to port splitters, hubs, switches, routers, wireless access points, multi-homed PC's and packet/data monitoring equipment/software.

Patients and visitors must not attempt to make any connection to the Trust's network via the fixed data ports.

## **6 Guidance for patients and visitors**

Guidance to help patients and visitors access the internet and social media sites in accordance with this policy will be made available on request and visible in public areas.

The Trust does not provide any form of technical support for patients or their visitors.

## **7 Review arrangements**

This policy will be reviewed in 3 years of the approval date, or sooner if required. The document will be reviewed in light of feedback, changing policy and guidance, and learning and review.

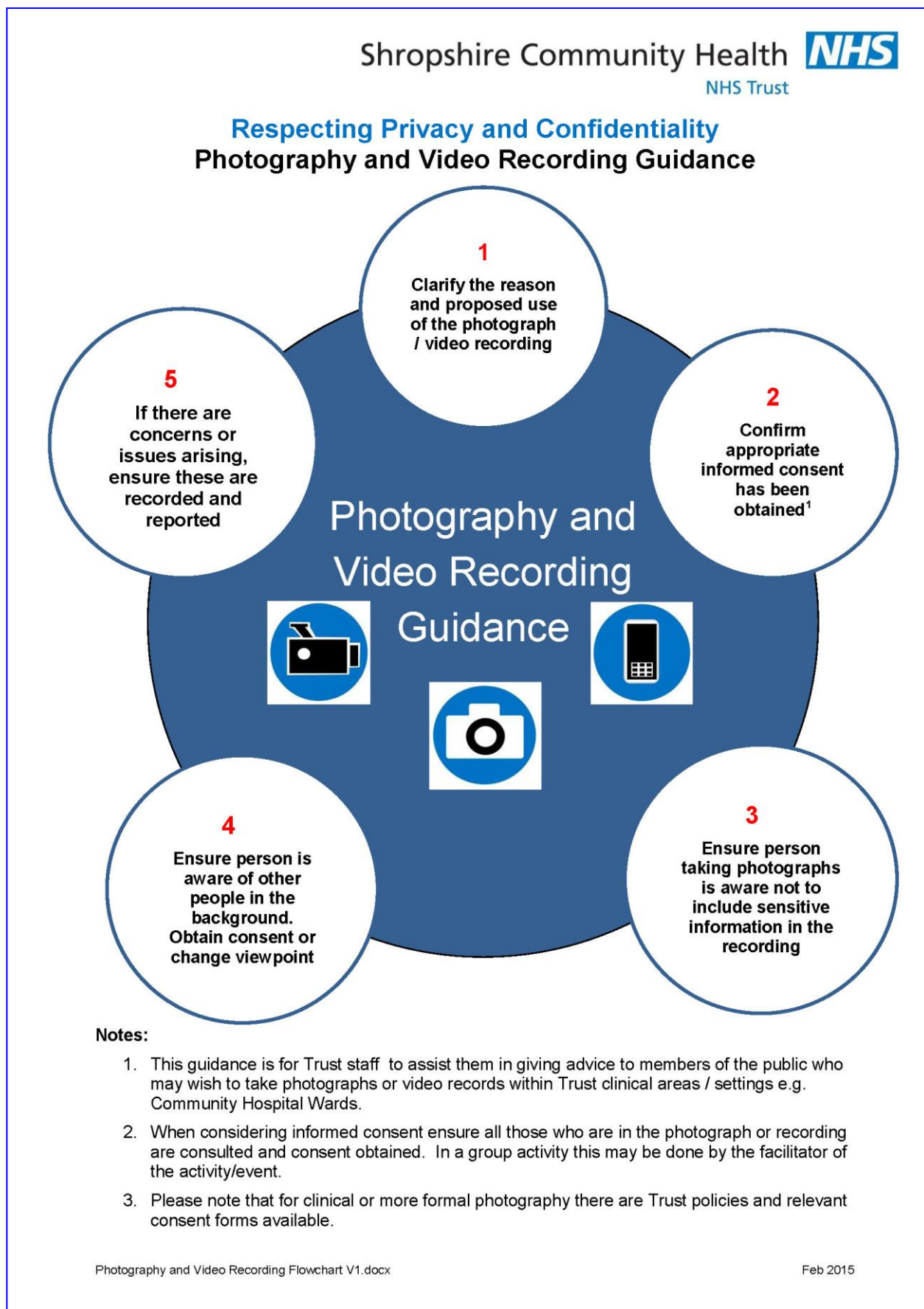
## **8 Associated documents**

Related Trust policies, procedures and guidelines include:

- Confidentiality Code of Practice
- Social Media Guidelines
- Media Policy and Procedure
- Guidance on the Safe Use of Mobile Phones and other Mobile Communication Devices in Clinical Areas
- Best Practice Guidance for Mobile Devices (phones and tablets)
- Clinical Photography Guidelines
- Patient and Public Information Policy
- Information Security Policy
- Information Governance Policy



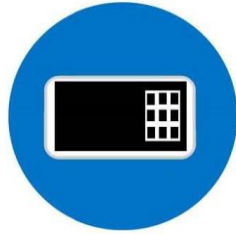
## Appendix 1





## Appendix 2

# Respecting Privacy and Confidentiality



Please note that this is a clinical area and we would ask that you respect people's privacy and confidentiality if you wish to take any photographs or video recordings. Please consider who and what may be included in any photograph or recording you take.

If in doubt please consult with a member of staff for assistance and/or guidance

# Treating Confidential Information with Respect