Leicestershire Partnership NHS Trust

Social Media and Electronic Communications Policy

This policy aims to provide guidance for employees, contractors, volunteers and the Trust as a whole in the safe use of social media and electronic communications. It also provides guidance on expectations of patients, carers and visitors within the Trust and what staff can do in relation to managing this.

Key Words:	Social Media; Electronic; Communications	
Version:	1.0	
Adopted by:	Trust Policy Committee	
Date this version was adopted:	31 March 2021	
Name of Author:	Head of Data Privacy/Data Protection Officer	
Name of responsible Committee:	Data Privacy Committee	
Please state if there is a reason for not publishing on website:	Not Applicable	
Date issued for publication:	March 2021	
Review date:	September 2023	
Expiry date:	31 July 2024	
Target audience:	All Staff, contractors, temporary staff, volunteers, patients, visitors	
Type of Policy	Clinical √	Non Clinical √
Which Relevant CQC Fundamental Standards?	Regulation 10 – Privacy and Dignity; Regulation 13 – Safeguarding service users from abuse and improper treatment; Regulation 17 – Good Governance	

Contents

Version Control and Summary of Changes

Version number	Date	Comments (description change and amendments)
V0.1	11 Nov 2020	First draft version of a brand new policy that supersedes the previous Internet and Electronic Communications Policy v2.0
1.0	March 2021	Final draft version for approval following extensive consultation

For further information contact:
Head of Data Privacy - *LPT-DataPrivacy@leicspart.nhs.uk*

Equality Statement

Leicestershire Partnership NHS Trust (LPT) aims to design and implement policy documents that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others. It takes into account the provisions of the Equality Act 2010 and promotes equal opportunities for all. This document has been assessed to ensure that no one receives less favourable treatment on the protected characteristics of their age, disability, sex (gender), gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy and maternity.

Due Regard

LPT will ensure that Due regard for equality is taken and as such will undertake an analysis of equality (assessment of impact) on existing and new policies in line with the Equality Act 2010. This process will help to ensure that:

- **Strategies, policies and procedures and services are free from discrimination;**
- **LPT complies with current equality legislation;**
- **Due regard is given to equality in decision making and subsequent processes;**
- **Opportunities for promoting equality are identified.**

Please refer to due regard assessment (Appendix 4) of this policy

Definitions that apply to this Policy

Sending	Dispatch a request or order, submitted by electronic means via email or web form
Posting	Electronic communication through websites
Downloading	Copying (data) from computer to another over the internet
Sharing	Exchange of data between organisations, technologies and people
Social Media	Computer based technology that facilitates the sharing of ideas, thoughts, and information through the building of social networks and communities
Electronic Communications	A communication sent via electronic means, including electronic posting, transmission to any number, address or internet website
Libellous	A piece of writing that contains bad and false statements about a person
Defamatory	Remarks or writing etc, that damage the good reputation of someone
Harrassment	Unwanted behaviour that it found to be offensive or makes a person feel humiliated or intimidated
Applications	Software that performs specific tasks for the end user
Overt	Shown openly/transparent
Covert	Not openly acknowledged or displayed
Streaming	A method of transmitting or receiving data over a computer network as a steady, continuous flow, allowing playback to start while the rest of the data is being received.

1.0 Purpose of the Policy

The policy has been developed to ensure staff, contractors, temporary staff, volunteers, patients/service users and visitors are aware of the need to use social media and electronic communications (including their associated mobile devices/technology) responsibly.

The policy aims to promote and protect patient and staff confidentiality, safeguarding privacy and dignity, and to protect the Trust from any reputational risk.

The policy applies to all staff groups (whether permanent, temporary or voluntary) as well as patients and visitors to the Trust whilst in clinical areas on Trust property, except for forensic services where local policy/procedure specifically prohibits the use of mobile communication devices/technology.

This policy does not apply to patients/service users private dwellings or other public areas as the Trust does not have control over these environments and for domestic private dwellings data protection does not apply as processing in these areas is classed a 'domestic purposes'.

2.0 Summary and scope of policy

The scope of the policy covers the use of mobile devices/technology to record staff, record consultations by patients/service users, sharing of ideas and creating communities, and using electronic means to access and share best practice.

The policy also outlines the expectations as specifically relating to persons detained under the Mental Health Act 1983.

When using social media staff (including temporary) need to remember:

- The use of camera facilities on mobile devices or any other such technology by employees, volunteers or contractors to take images of the workplace and then load on to personal social media sites is not permitted. Any images taken during the course of their work for therapeutic or promotional purposes must not be taken on personal devices and must have received prior approval and informed consent sought for those who are the subject of the images and shared on work related social media accounts;
- Patients/service users and visitors must be informed of the policy and their expectations with regard to using social media and electronic communications on Trust premises through the provision of information leaflets;
- Patients/Service users are not allowed to capture images or information for use on social media of other patients/service users and staff, or within our buildings (particularly in relation to information governance), without their express informed consent.
- Ensure that they behave in a manner that is consistent with the Trust's expectations regarding the duty of care and confidentiality they owe to colleagues;
- Patient/service user privacy and dignity along with safeguarding principles must also be adhered to;

- They will be held accountable for any information published/posted which may compromise themselves within the realms of their role and responsibilities as an employee or volunteer of the Trust and/or compromise their colleagues and/or the Trust;
- They not permitted to access social media sites for personal use through the use of Trust devices, with the exception of accessing the Trusts' official Facebook, Twitter or Instagram accounts. Exceptions are where access these sites for work use, such as networking with other professionals across the country, to learn and share good practice.

3.0 Introduction

The aim of this policy is to provide guidance to all staff (temporary, permanent or voluntary), patients/service users and visitors with guidance on the safe and appropriate use of social media and electronic communications (including any associate devices/technology to enable this).

The Trust recognises that with advancements in technology the use of mobile/web and recording enabled devices there is a significant increase in the use of social media and electronic communications.

Social media and electronic communications can be beneficial to an organisation to engage with patients, stakeholders and to deliver key messages to staff groups and volunteers. It is also acknowledged that patients/service users and staff use social media and electronic communications in their personal lives.

For the purpose of this policy the reference of social media is inclusive of the use of social networking and electronic communications refers to the sending, posting, downloading or otherwise sharing of digital information. The detailed definitions of both can be found in the definitions section of this policy.

4.0 Duties within the Organisation

4.1 The Trust Board has a legal responsibility for Trust policies and for ensuring that they are carried out effectively.

4.2 The Trust Policy Committee is mandated on behalf of the Trust Board to adopt policies

4.3 The Data Privacy Committee holds the responsibility for the monitoring and review of this policy

4.4 Divisional Directors and Heads of Service are responsible for:

- Ensuring that their Managers and Team Leaders are aware of this policy and have supplemented this with any appropriate local procedures.

4.5 Managers and Team leaders are responsible for:

- Ensure that their staff, any contractors/temporary workers or volunteers in their areas of work are aware of this policy and the good practice guidance

within it.

4.6 Responsibility of Staff

- All staff, including contractors, temporary workers and volunteers comply with the expectations of this policy to support the reputation of the Trust and their profession.

- **Patients/service users and visitors must be informed of the policy and their expectations with regard to using social media and electronic communications on Trust premises through the provision of information leaflets.**

4.7 Registered professional including medial staff

- Should be aware and familiarise themselves with the guidance issued by their relevant professional bodies i.e. British Medical Association (BMA), Nursing & Midwifery Council (NMC) and Health and Care Professionals Council (HCPC).

5.0 Social Media

5.1 Principles of use

- When using social media employees (including contractors, temporary or voluntary), patients/service users and visitors must ensure that they behave in a manner that is consistent with the Trust's expectations regarding the duty of care and confidentiality they owe to colleagues, patients/service users and the organisation. Patient/service user privacy and dignity along with safeguarding principles must also be adhered to.

- Information once published on the internet by an employee, volunteer, patient/service user or visitor is no longer considered private. They will therefore be held accountable for any information published/posted which may compromise themselves within the realms of their role and responsibilities as an employee or volunteer of the Trust and/or compromise their colleagues and/or the Trust. **Volunteers, patients/service users and visitors may also find that they have breached the Human Rights Act 1998 with regards to breaching respect for private and family life as set out in Article 8 of the European Convention on Human Rights. This may leave individuals open to criminal or civil court proceedings.**

- **The use of camera facilities on mobile devices or any other such technology by employees, volunteers or contractors to take images of the workplace and then load on to personal social media sites is <u>not permitted</u>.** Any images taken during the course of their work for therapeutic or promotional purposes must not be taken on personal devices and must have received prior approval and informed consent sought for those who are the subject of the images and shared on work related social media accounts.

- Employees, contractors and volunteers are responsible for their own online behaviours and must ensure they avoid online actions or content that is inaccurate, libellous, defamatory, harassing, threatening or in any other way illegal. Failure to do so may result in disciplinary action, criminal or civil proceedings.

- When registering for any social media applications for personal use, the Trust email address must not be used, unless it relates to NHS promotional benefits but care must be taken with the website cookies to ensure that these are linked to your work account.

- Any social media accounts on behalf of LPT or LPT services must be approved by the communications team, who will consider if this is appropriate, and monitor and log the account. This is within the remit of reputational risk and appropriate representation of LPT. These accounts must remain apolitical and professional at all times.

5.2 Use of social media for personal use

Employees, contractors and volunteers are not permitted to access social media sites for personal use through the use of Trust devices, with the exception of accessing the Trusts' official Facebook, Twitter or Instagram accounts. It is acceptable to access these sites for work use, such as networking with other professionals across the country, to learn and share good practice.

Employees, contractors and volunteers who have the facility to access social media sites for personal use via their own mobile device/technology are reminded that they must limit this use and away from patient facing areas so as not to interfere with their working day and to limit use to allocated break times. Failure to do so may lead to disciplinary action and a referral could also be made to the Local Counter Fraud Specialist (LCFS) for investigation in accordance with the Trusts Fraud, Bribery and Corruption Policy. LCFS investigations may lead to the application of a criminal sanction.

Employees, contractors and volunteers must not breach the confidentiality of patients/services users or colleagues and must act in accordance with Trust policies and their own Professional Code of Conduct for the safe and secure use of personal information.

Employees, contractors and volunteers must not act in a way that will bring the Trust into disrepute or adversely impact its reputation.

Personally expressed opinions and/or information shared via social media by employees are the expressed opinions of themselves as individuals and do not reflect those of the Trust. This must be stated on any profile biographies, especially if your job role or employer is specified in it.

Patients/Service users are not allowed to capture images or information for use on social media of other patients/service users and staff, or within our buildings (particularly in relation to information governance), without their express informed consent as this may impinge on their Human Rights, the Data Protection Act 2018 (DPA18) and the UK General Data Protection Regulation (UK GDPR) 2020. Safeguarding issues may be raised in some circumstances.

Employees, contractors and volunteers should take care not to pursue personal relationships with patients/service users and visitors by means of social media, ensuring that professional boundaries are maintained and protected.

Where a patient/service user makes contact staff via social media, this should be reported to their line manager and where this relates to clinical care, it should be recorded in their clinical record. Staff should remind the patient/service user of the appropriate channels of communication for clinical purposes. See Appendix 5 for guidance around dealing with abusive images.

Professional communication via social media with patients/service users must only take place via sites that have received approval and authorisation of the Communications Team. The standard of the communication should meet Trust Records Keeping Standards as well as relevant professional bodies' standards.

Employees, contractors, volunteers and patients/service users must be mindful of the content they share via the internet and the implications thereof. This includes written and photographic images.

Professional communication and use of social media to engage with patients/service users must be done so only with their express informed consent. Consent forms for photography are available from the communications team.

5.3 As a Communication Tool

The Trust will use social media when appropriate for example to promote the services of the organisation, engage with and provide support to specific patient/service user groups and provide a platform to enable others to provide feedback and comment. This is an expectation of service users and the general public in terms of engagement and transparency.

The use of video clips/streaming may be an appropriate method of providing advice, support and guidance communication for staff groups or patient/service users groups. Access to sites such as YouTube can be found on the LHIS Applications approved list. Any films must be shared with the communications team for approval and appropriate upload to LPT's website and youtube channel.

Creation of any social media accounts for professional use must be done via the appropriate authorisation process to the Communications Team.

The participation of patients/service users for any social media platform for professional use must be done so with their express informed consent.

Good Practice Guidelines for Social Media as provided by the Trust and any relevant Professional Code of Conduct must be adhered to at all times.

5.4 Risks

5.4.1 Unauthorised Disclosure of Personal and Business Information
The use of social media sites can provide an easy means for personal, sensitive or confidential information to be leaked from an organisation. This may be unintentional or malicious. Once information is loaded onto a social media platform it enters the public domain and can be viewed, stored, processed and shared globally.

This can result in a breach of confidentiality, disciplinary action, criminal or civil proceedings, loss of reputation and business plus financial penalties.

5.4.2 Identity Theft
Most social media platforms/sites allow users to create personal profiles. It is possible for individuals to place large amounts of personal information within their profiles which may be of use to criminals and others seeking to steal and reuse identities for their own financial or other gain. The examples of information that can be stored on a personal profile are: full names, dates of birth, address, telephone contacts, religion, ethnicity, nationality, employer and photographs, all of which can be used to clone your identity. Note that information and guides on privacy settings are available on StaffNet and from the communications team.

5.4.3 Reputational Damage
Comments that are left on sites that are unjustified, inaccurate or ill-considered may adversely affect the public and professional opinion towards a patient/service user or employee. This includes any photography that doesn't role model our expected high standards at LPT. This can lead to reputational damage of an individual or an organisation and can result in disciplinary action, civil and/or criminal proceedings.

5.4.4 Damage to End User Devices
The definition of an end user device includes PC's, laptops, tablets, smartphones and other hardware that end users can use to interact with data and applications.

The downloading and installation of unauthorised applications may adversely affect the operating systems or application codes of the Trusts' devices. Malicious viruses

may be contained within such applications.

More detail on the approval process can be found in the Trusts Information Security and Risk Policy.

5.4.5 Intimidation, Harassment or Threat
Strong views that are shared via social media can offend and cause the reader anxiety, distress and/or personal safety issues. Individuals may feel threatened, bullied, harassed or intimidated by comments or images shared via social media.

Please see Appendix 5 for Guidance on Dealing with Abusive Images and associated flowchart, and Appendix 6 for identifying Threat and associated flowchart on how the steps to be taken to deal with this.

5.4.6 Breach of Legislation
When an organisation or an individual acting for non-domestic purposes, posts personal information on social networking platforms/sites, they will need to ensure that they have complied with DPA18 and UK GDPR. The same applies if they download personal information from a social networking platform/site for non-domestic purposes.

Article 8 of the Human Rights Act 1998 stipulates that everyone has the right to respect for their private and family life, home and correspondence. This right is subject to proportionate and lawful restrictions. Unauthorised disclosure of personal information can lead to a breach of this Act.

Other legislation that may be relevant in the misuse of social media are:

- Protection from Harassment (NI) Order 1997
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Computer Misuse Act 1990
- Copyright, Designs and Patent Act 1988
- Copyright (Computer Programs) Regulations 1992
- The Terrorism Act 2000
- Official Secrets Act 1911-1989
- Obscene Publications Act 1994

6.0 Devices and Recording

6.1 Confidentiality, Privacy and Dignity

Patient/Service user confidentiality and safety is the primary consideration when

mobile devices/technology are used to make recordings within clinical areas. Any video, image or audio recording made on Trust premises which contains reference to any patient/service user within a clinical setting without their express informed consent may be an interference with that individual's right to privacy under Article 8 of the Human Rights Act 1998.

In accordance with this, any person who has access to a device/technology with recording capability in a clinical setting, must not use the recording functionality in any area where patient/service user confidentiality may be infringed upon such as any communal areas. Staff must also take account of their environments when recording or photographing, to ensure there are no information governance breaches such as names of patients on boards, or clinical records on show.

6.2 Appropriate Use of Mobile device/technology by Patient/Service users, visitors or staff

Whilst it is important that patients/service users are able to use their mobile devices to maintain essential support networks and ties with friends and family, it is important that the use of mobile communication and recording devices/technology within the Trust is managed to ensure that patient/service user confidentiality is maintained and the use of mobile devices/technology is not abused.

This is to protect and preserve the privacy, dignity and safeguarding issues of all individuals including patients/service users, visitors and staff. Staff should be aware that many devices/technologies contain cameras and that images can be uploaded immediately to a range of social media sites/platforms. Posters are available to display in patient areas to remind patients to not record or photograph in our buildings, including any other patients or our staff.

Staff should ensure that personal mobile communication devices/technology are not used in any clinical or in-patient areas where they may disturb others or interfere with the provision of care. Devices/technology left in staffroom lockers should be turned off or set to silent to avoid disturbance, and community staff should ensure that personal devices should be switched to 'silent' or 'vibrate' whilst on duty.

Where staff are required to use a mobile device/technology to take images of a patient/service user on a ward or in the community, for any purpose such as the monitoring and management of wound care, only mobile devices/technology supplied by the Trust can be used for this purpose, personal mobile devices/technology must not be used for processing this information.

Mobile devices/technology may be used within in-patient setting in the following circumstances:

1. Trust provided devices:
   - Where local operational policy permits the managed use of mobile devices/technology by staff;
   - By staff in WIFI-enabled designated areas for accessing emails and clinical information systems;
   - Where there is a clinical imperative that negates the use of all other means of communication.

2. Personal devices
   - Where local operational policy permits the managed use of mobile devices/technology by patients/service users or contractors;
   - Where clinical staff and managers have identified that they may need to be urgently contacted and this has been agreed by the most senior staff on duty;

6.3 Persons detained under the Mental Health Act 1983

Persons detained under the Mental Health Act have the same rights as informal persons to having contact with family and friends under Article 8 of the Human Rights Act, namely the right to private life. As such mobile devices/technology need to be readily accessible.

The Mental Health Act Code of Practice 2015, Chapter 8 Privacy, Safety and Dignity deals with detained person's access to mobile communication devices/technology (including access to the internet and social media) recognising that hospital managers have implied powers over detained individuals rights to their access and use and it may therefore be permissible following an individual risk assessment to restrict the use of mobile communications devices/technology. However the principle that should underpin any local policy/procedure on the use of such devices is that detained individuals are not free to leave the premises but their freedom to communicate with friends and family should be maintained as far as possible and restricted to the minimum extent necessary.

Restrictions need to be a proportionate response, and pursuant to the legitmacy of protecting the health and safety of the patients/services users and others, and clearly communicated to patients. Alternative options must be considered and valid reasons for restrictions demonstrated in the patient/service users records.

The clinical team may therefore restrict the use of mobile communication devices/technology of patients/service users who are deemed not to have capacity to manage the identified risk for the duration of time that the risk exists. This should be clearly outlined in their care plan and be reviewed during the clinical team reviews.

Risk include the use of the device/technology to access inappropriate numbers or receiving inappropriate calls/messages, placing themselves and others at risk, in terms of abuse, emotional distress, or the use of numbers with a high cost, to safeguard the patient/service user.

7.0 Recording of Staff

7.1 The Law

There are no specific legal requirements that govern an individual making a personal recording of their medical/health related consultation or treatment, either overtly or covertly for their private use. Recordings made to keep a personal record of what a healthcare professional said are deemed to constitute 'note taking' and are therefore permitted when undertaken for this purpose. Whilst a patient/service user does not require permission to record their consultation, common courtesy would suggest that permission should be sought by the patient/service user in most cases.

The content of the recording is confidential to the patient/service user, not the healthcare professional. The patient/service user can waive their own confidentiality as they wish; this could include disclosing the details of their consultation with third parties or even posting and/or sharing the recording in unadulterated form on the internet through social media sites/platforms.

The position may, however, change once a recording is no longer used as a record of consultation, for example where the recording is disclosed or publicised in a modified way which is not connected to the consultation. This could include an instance where it is designed to cause distress to or harass another individual captured in the recording. Any such disclosure or publication, depending on the nature and context, may attract a civil action for damages and may also be a criminal offence.

- UK GDPR – The recording of a consultation is likely to constitute processing of personal data under DPA and as such it has to comply with the provisions of UK GDPR. There is an exemption in the DPA where personal data is processed by an individual for their own purpose. In such cases, the 'processing' does not engage data protection principles (the 'domestic purposes' exemption. However, further processing of the information is likely to have to comply with the DPA.

- Potential legal action – If any part of an overt or covert recording of the patient/service users consultation or members of the public, visitors or relatives is disclosed to a third party without the prior consent of the other recorded parties, then depending on the nature and context of such disclosure, a criminal offence may be committed, civil legal action may be taken, or breach of UK GDPR may occur.

7.1.1 Criminal Offences

Criminal offences may arise out of unauthorised disclosure of recordings depending on how that disclosure or publication is made. However, the most likely offences could include an offence contrary to Section 1 of the 'Protection of Harassment Act'1997; an offence contrary to Section 4, 4a, or 5 of the 'Public Order Act' 1986; an

offence contrary to Section 1 of the 'Malicious Communications Act' 1988; or an offence contrary to Section 127 of the 'Communications Act' 2003.

- Protection of Harassment Act 1997 – it is an offence under this Act to cause distress and upset to an individual knowing that such action will cause distress and upset. This could apply if any individuals use the act of recording with the known intention to cause distress and upset.

- Criminal Justice and Immigration Act 2008 – If an individual is clearly recording with the intention to cause a nuisance then they be committing an offence under this Act under section 119. This applies to persons who are not seeking medical advice, treatment or care who could commit the offence if they, for example, use a mobile phone in such a way to cause a nuisance or disturbance to an NHS staff member and where they fulfil the other elements of the offence (subject to certain safeguards set out in the Act).

- Defamation – Actions for libel can be brought in the High Court for any published statements which are alleged to defame a named or identifiable individual (or individuals; under English Law companies are legal persons, and allowed to bring suit for defamation) in a manner which causes them loss in their trade or profession, or causes a reasonable person to think worse of him/her/them. A statement can include an implication; for instance, a photograph or image in a particular context (for example a photograph with an accompanying headline implying wrong doing or incompetence) could be held as a personal allegation about the individual featured in the photograph.

This is not an exhaustive list and the specific offence charged would depend on the facts. See Appendix 6 for further information and guidance.

7.2 Overt recordings by patients/service users

Although we cannot place restrictions on a patient/service user wishing to record notes of a consultation or conversation with a health professional, where it is felt absolutely necessary to do so, we should ensure that:

- Any recording is done open and honestly
- The recording process itself does not interfere with the consultation process, treatment or care being administered
- The patient/service users is made aware that a note will be made in their health record stating that they had recorded the consultation or care being provided
- The patient/service user is reminded of the private and confidential nature of the recording and it is their responsibility to keep it safe and secure
- Any recording is made for personal use
- Patients/service users are aware that the misuse of a recording may result in criminal or civil proceedings
- Patients/service users are discouraged from making recordings in the first place, unless it is deemed absolutely necessary by highlighting the above responsibilities

7.3 Covert recordings by patients/service users

Although we cannot place restrictions on a patient/service user wishing to record notes of a consultation or conversation with a health professional covertly, where staff are aware that covert recording is a significant issue they should aim to discourage them from doing so by ensuring that:

- The Trust promotes the open and honest recording of consultations where a patient/service user deems it absolutely necessary (see the above advice which applies equally to covert recording)
- Patients/service users are aware that the Trust takes proactive steps to investigate and address any issues regarding patient/service user treatment and care, to avoid them feeling it necessary to record their consultation
- Relevant staff should consider providing patients/service users with a written record summary, and or a verbatim record (if practical) of their consultation for their personal use
- Patients/service users are advised that they are entitled to see their records, if they wish to, by informally asking their healthcare professional in charge of their care, or to request a copy of their records formally through making a Subject Access Request (SAR) under DPA18 and UK GDPR. They can make an application through the Trust website.
- Patients/service users are given information on how they can complain if they have issues with their care and treatment, and their attention is drawn to the relevant guidance from the Care Quality Commission (CQC) and Information Commissioners Office (ICO).

7.4 Recording in a Hospital Setting

- Patients/service users and the public are not permitted to make recording or take images within a hospital setting without any prior agreement from a senior manager on site, this includes in-patient and clinic areas. Any agreed recording must be supervised to ensure no peripheral individuals are captured in recordings.

- The Trust has a duty to safeguard patients/service users privacy and dignity and therefore any such actions involving the recording should be stopped and images deleted.

- If individuals refuse to stop recording or delete images after being asked, they should be told that they will be reported to the police and potential criminal sanctions sought. They will also be subject to immediate exclusion from Trust premises and further permanent exclusions could be applied. These individuals must be told that if they publish images or share with third parties in any way they will be committing an offence and the Trust may take legal action.

- If unauthorised filming actions become aggravated security must be called and the police where necessary.

7.5 Unauthorised Image or audio recordings

If there is a reason to believe that unauthorised recordings have been taken by a

patient/service user, staff need to make the most senior member of staff on duty aware of their belief and then under the direction of the nurse in charge or unit manager ask for the mobile device/technology to be handed over to Trust staff for recordings to be deleted. It should be made clear that this is being done because there are concerns for confidentiality, privacy and dignity of others.
It may be that the patient/service user or visitor chooses to delete the images themselves under the supervision of staff.

If the device is handed over to staff the device user/owner should remain with it to prevent allegations of damage or misuse.

If the person using the mobile communications device/technology is unwilling to delete the images or to hand over the devices they have used to make the recordings, they should be requested to remain in the presence of staff until a senior manager can attend.
Please note: *that it is not appropriate to detain any person against their will or take from them a mobile communications device they are unwilling to hand over.*

The staff member must ask that the person does not send the images held on the mobile device to any other device. If they suspect that this has happened the manager for the area must be informed immediately.

Staff should ask for a list of any person(s) to whom images/recordings have been sent including their contact details. This should also include any social media sites/platforms to which images/recordings have been sent. This information will be forward to the Local Security Management Specialist (LSMS) and an incident raised. Consideration must be given to whether this would constitute a Serious Incident.

It should be made clear from the outset that where appropriate the Trust will be instrumental in pursuing civil court action/criminal prosecution if the user breaches the right of others or commits an offence.

Where a patient/servicer user has contravened the requirements of this policy, or repeatedly threatened to make recordings contravening this policy, it may be appropriate that as a condition of their continued treatment their mobile communication device is placed in safe storage and used only on request in designated areas under supervision. This must be considered by the clinical team and recorded in the patient/service users record. A person's privacy and dignity whilst using the mobile communications device must be respected at all times.

Where a member of staff has contravened this policy, their Line Manger will implement the Supporting Performance Policy.

Where a volunteer has contravened this policy, the Voluntary Services Manager will

be notified immediately.

Visitors and relatives who contravene this policy may have their rights to visit Trust premises reviewed by the Service Director and clinical team.

8.0 Training needs

There is no training requirement identified within this policy, however there are social media guidelines and best practice guides on how to use social media on StaffNet Please see the references in section 11.0

9.0 Monitoring Compliance and Effectiveness

Ref	Minimum Requirements	Evidence for Self-assessment	Process for Monitoring	Responsible Individual / Group	Frequency of monitoring
15	Note made of recording of consultation or treatment in records	7.2	Record Keeping Audit	Clinical Effectiveness Group	Annually
17	Unauthorised recording incident reported	7.5	Caldicott Report	Data Privacy Committee	Quarterly
9	Recording is undertaken with express consent	5.5	Record Keeping Audit	Clinical Effectiveness Group	Annually

10.0 Standards/Performance Indicators

TARGET/STANDARDS	KEY PERFORMANCE INDICATOR
CQC Regulation 10 – Privacy and Dignity	
CQC Regulation 13 - Safeguarding service users from abuse and improper treatment	

11.0 References and Bibliography

The policy was drafted with reference to the following:

Use of Electronic Communication with Service Users Policy
Data Protection and Information Sharing Policy
Information Security and Risk Policy

HCPC Guidance on the use of social media
https://www.hcpc-uk.org/registration/meeting-our-standards/guidance-on-use-of-

social-media/
NMC Guidance on social media
https://www.nmc.org.uk/standards/guidance/social-media-guidance/
BMA Ethics of Social Media Use
https://www.bma.org.uk/advice-and-support/ethics/personal-ethics/ethics-of-social-media-use
BMA Ethics Toolkit for Medical Students on Social Media
https://www.bma.org.uk/advice-and-support/ethics/medical-students/ethics-toolkit-for-medical-students/social-media

Trust Social Media Guidance and Tools
https://staffnet.leicspart.nhs.uk/support-services/communications/social-media-guidance/

Human Rights Act - https://www.legislation.gov.uk/ukpga/1998/42/contents
Data Protection Act 2018 -
https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
UK General Data Protection Regulations -
https://www.legislation.gov.uk/ukdsi/2019/9780111177594/pdfs/ukdsi_9780111177594_en.pdf

Appendix 1

The NHS Constitution

The NHS will provide a universal service for all based on clinical need, not ability to pay. The NHS will provide a comprehensive range of services

Shape its services around the needs and preferences of individual patients, their families and their carers	☐
Respond to different needs of different sectors of the population	☐
Work continuously to improve quality services and to minimise errors	☐
Support and value its staff	x
Work together with others to ensure a seamless service for patients	☐
Help keep people healthy and work to reduce health inequalities	☐
Respect the confidentiality of individual patients and provide open access to information about services, treatment and performance	x

Appendix 2

Stakeholders and Consultation

Key individuals involved in developing the document

Name	Designation
Kamy Basra	Head of Communications
Debbie Bromley	Safeguarding Practitioner
Jacqui Newton	
Neil King	Trust Lead for Safeguarding

Circulated to the following individuals for comment

Name	Designation
Michelle Churchard	Head of Nursing, Directorate of Mental Health
Gordon King	Service Director, Directorate of Mental Health
Avinash Hiremath	Medical Director, Caldicott Guardian
Girish Kunigiri	Consultant Psychiatrist/Chief Clinical Information Officer
Safeguarding Team	
Data Privacy Committee members	
Helen Perfect	

Appendix 3

Due Regard Screening Template

Section 1	
Name of activity/proposal	Social Media & Electronic Communications Policy
Date Screening commenced	November 2020
Directorate / Service carrying out the assessment	Enabling/Data Privacy
Name and role of person undertaking this Due Regard (Equality Analysis)	Sam Kirkland, Head of Data Privacy/Data Protection Officer
Give an overview of the aims, objectives and purpose of the proposal:	
AIMS: The aim of the Policy is to set out the parameters around the use of social media and electronic communications for all groups of staff including temporary and patients/service users	
OBJECTIVES: • To be clear on when it is permitted to use social media and electronic communications and when not; • Set out the rules in which we are working in; • Protect those using social media legitimately and provide guidance on actions when it is not	

Section 2	
Protected Characteristic	**If the proposal/s have a positive or negative impact please give brief details**
Age	Neutral
Disability	Neutral
Gender reassignment	Neutral
Marriage & Civil Partnership	Neutral
Pregnancy & Maternity	Not Applicable
Race	Neutral
Religion and Belief	Neutral
Sex	Neutral
Sexual Orientation	Neutral
Other equality groups?	

Section 3			
Does this activity propose major changes in terms of scale or significance for LPT? For example, is there a clear indication that, although the proposal is minor it is likely to have a major affect for people from an equality group/s? Please tick appropriate box below.			
Yes		No	
High risk: Complete a full EIA starting click here to proceed to Part B		Low risk: Go to Section 4.	√

Section 4
If this proposal is low risk please give evidence or justification for how you reached this decision:
The Policy aims to set out the most common circumstances and is applicable to individuals of all groups

Signed by reviewer/assessor	Sam Kirkland	**Date**	25/02/21
Sign off that this proposal is low risk and does not require a full Equality Analysis			
Head of Service Signed	Sam Kirkland	**Date**	25/02/21

Appendix 4

DATA PRIVACY IMPACT ASSESSMENT SCREENING

Data Privacy impact assessment (DPIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet Individual's expectations of privacy.
The following screening questions will help the Trust determine if there are any privacy issues associated with the implementation of the Policy. Answering 'yes' to any of these questions is an indication that a DPIA may be a useful exercise. An explanation for the answers will assist with the determination as to whether a full DPIA is required which will require senior management support, at this stage the Head of Data Privacy must be involved.

Name of Document:	Social Media and Electronic Communications Policy	
Completed by:	Sam Kirkland	
Job title	Head of Data Privacy	**Date** 25/02/2021

Screening Questions	**Yes / No**	**Explanatory Note**
1. Will the process described in the document involve the collection of new information about individuals? This is information in excess of what is required to carry out the process described within the document.	No	
2. Will the process described in the document compel individuals to provide information about them? This is information in excess of what is required to carry out the process described within the document.	No	
3. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information as part of the process described in this document?	No	
4. Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	No	
5. Does the process outlined in this document involve the use of new technology which might be perceived as being privacy intrusive? For example, the use of biometrics.	No	
6. Will the process outlined in this document result in decisions being made or action taken against individuals in ways which can have a significant impact on them?	No	
7. As part of the process outlined in this document, is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For examples, health records, criminal records or other information that people would consider to be particularly private.	No	
8. Will the process require you to contact individuals in ways which they may find intrusive?	**No**	

If the answer to any of these questions is 'Yes' please contact the Data Privacy Team via Lpt-dataprivacy@leicspart.secure.nhs.uk
In this case, ratification of a procedural document will not take place until review by the Head of Data Privacy

Data Privacy approval name:	Sam Kirkland, Head of Data Privacy
Date of approval	26/02/21

Acknowledgement: This is based on the work of Princess Alexandra Hospital NHS Trus

Appendix 5

Dealing with Abuse Images - Guidance

Definition of "digital" http://llrscb.proceduresonline.com/index.htm	Digital applies to data carrying signals which carry electronic or optical pulses
Definition of "technology" http://llrscb.proceduresonline.com/index.htm	Technology covers a range of electronic tools: use has become more widespread through the Internet being available using text, photos and video. The internet can be accessed on mobile phones, laptops, computers, tablets, webcams, cameras and games consoles
Definition of "abuse images" http://llrscb.proceduresonline.com/index.htm	Any indecent, obscene image involving a child has, by its very nature, involved a person, who in creating that image, has been party to abusing that child. For the purpose of this guidance the term 'Abuse Images' will also be applied to adults where coercion, control and harm has been, or is being perpetrated against an adult. This also may include 'revenge porn' whereby following the ending of a relationship, consensual sexual images taken during the relationship are shared via the internet and/or social media (see also section 'What about images of adults?'

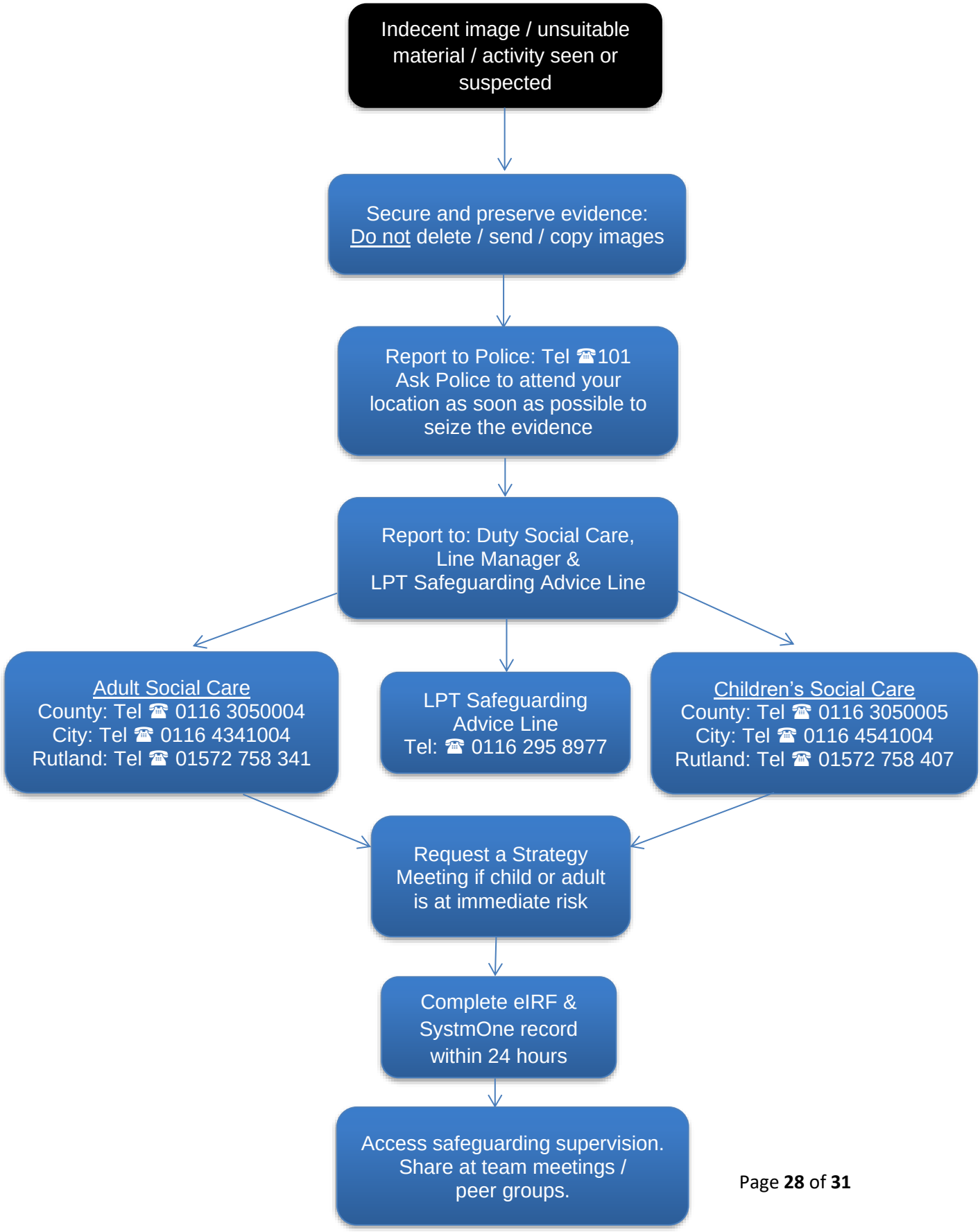
Definition of "indecent images of children" https://www.cps.gov.uk/legal-guidance/prohibited-images-children	Indecent Images of Children are: • The performance by a person of an act of intercourse or oral sex with or in the presence of a child • An act of masturbation by, of, involving or in the presence of a child • An act which involves penetration of the vagina or anus of a child with a part of a person's body or with anything else; • An act of penetration in the presence of a child, of the vagina or anus of a person with a part of a person's body or with anything else • The performance by a child of an act of intercourse or oral sex with an animal (whether dead or alive or imaginary) • The performance by a person of an act of intercourse or oral sex with an animal (whether dead or alive or imaginary) in the presence of a child. Prohibited Images of Children are non-photographic images (it includes computer generated images, cartoons, magna images and drawings). It excludes indecent photographs. The offence carries a maximum of 3 years imprisonment.

What the Law says https://www.cps.gov.uk/legal-guidance/indecent-images-children-iioc	• In the UK under the Protection of Children Act 1978 there is a strict prohibition on the taking, making, circulation and possession with a view to distribution of any indecent photograph or pseudo photograph of a child and such offences carry a maximum sentence of 10 years' imprisonment • There are defenses for those aged over the age of consent (16) who produce sexual photographs for their own use within a marriage or civil partnership; these defenses are lost if such images are distributed.
What about images of adults?	It is a criminal offence to share private sexual photographs or film without the consent of the person depicted. The footage needs to be classed as "obscene" rather than "offensive" and shared with the intent to cause them distress.
"Secure & preserve" is a term used by the Police to manage indecent images	As a practitioner it is your responsibility to contact the police on 101 and explain in detail what has been observed and request that they attend your location to seize the evidence as soon as possible. Leave device in situ, do not attempt to close down or copy any of the material to another device.

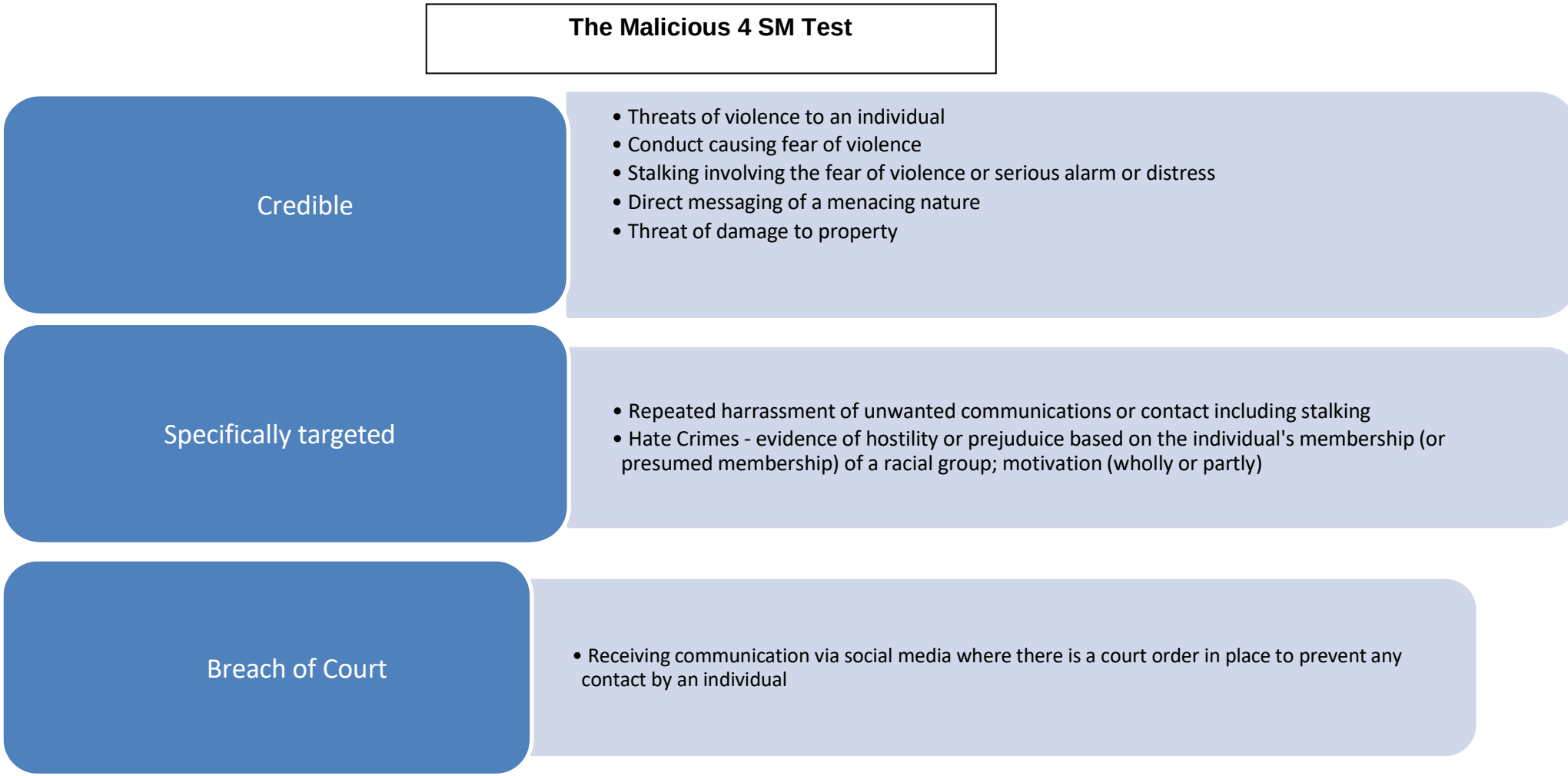
Can I be prosecuted for receiving/viewing images sent/shown to me by a patient/client?	If you follow the process below you will have done nothing illegal. If you receive an abuse image/s you should not share it or view it repeatedly. You must report it to the police and your line manager. You must also complete an eIRF. The police will guide staff regarding management of the image/s. This should include the police coming to the member of staff's place of work and collecting the phone/device. They will view the material themselves to establish whether there is a crime. They will plan a forensic investigation (i.e. gathering the data/looking for evidence regarding the location/who might be in the image/filming it). You should also contact the LPT safeguarding team as a matter of urgency.
Can I take photos of a patient if I consider it will enhance patient care?	Community staff may feel that a photo could enhance patient care e.g. positioning, use of sleep systems and pressure area management. Consent for this should be sought from the patient but if this is not possible a "best interest" decision should be made. It is preferable if the patient is not identifiable in the photo. The image can be sent by secure email and uploaded onto System One as an attachment. The photo must then be deleted from the mobile phone.

	For concerns of a non-accidental injury to a child (NAI), an urgent referral to social care should be made where a request for a medical should be sought and photographs would be taken during this process as a part of achieving best evidence (ABE).
Additional resources	
http://www.barnardos.org.uk/what_we_do/our_work/sexual_exploitation/what-is-cse/digital-dangers https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/share-aware/ https://www.youtube.com/user/ceop https://leics.police.uk/advice-and-information/information-zone/child-abuse/further-information-professionals https://swgfl.org.uk/services/professionals-online-safety-helpline	

DEALING WITH ABUSE IMAGES



Appendix 6


The Malicious 4 SM Test
Credible
• Threats of violence to an individual
• Conduct causing fear of violence
• Stalking involving the fear of violence or serious alarm or distress
• Direct messaging of a menacing nature
• Threat of damage to property
Specifically targeted
• Repeated harrassment of unwanted communications or contact including stalking
• Hate Crimes - evidence of hostility or prejuduice based on the individual's membership (or presumed membership) of a racial group; motivation (wholly or partly)
Breach of Court
• Receiving communication via social media where there is a court order in place to prevent any contact by an individual

Communications - Grossly offensive, obscene,	• The intention to send a communication which is grossly menacing. The test is: How much does it impact your reputational rights? • Intention will exist where there is a campaign i.e. it is repeated

The Public Interest Test

It is vitally important to consider the context and approach of the communication, as communications on social media often takes place in quite a different context than other traditional channels. Banter, jokes and offensive comments are commonplace and often spontaneous. These types of communications which are intended for just a small restricted audience may, through no fault of the author, reach countless individuals.

There is a balance here between what would be considered inhibiting or discouraging free speech and the legitimate exercise of natural and legal rights; and those which would meet a higher evidential threshold and may require prosecution.

The test is that there is sufficient evidence that the communication in question meets the criteria set out in the Malicious 4 SM Test above and is more than:

- Offensive, shocking or disturbing; or
- A satirical or rude comment or comment made as part of a campaign topic; or
- The expression of unpopular or unfashionable opinion about serious or trivial matters or banter or humour, even if it is distasteful to some or painful to those subjected to it

The issue can be whether the whole message or communication is grossly offensive, obscene or false. For example, an image that in itself falls short of being offensive or obscene may become offensive when considered in the context of the whole message (e.g. the circumstances in which it was sent or the people to whose attention it was brought).

Example of Grossly Offensive

An individual names an individual member of staff and that they have committed an indecent offence against someone of a racial group

Example of expression of free speech

An individual makes a derogatory comment about a named individual member of staff and how they have treated them An

individual makes some offensive comments about a group of staff e.g. nurses on a named ward