

# Use of Electronic Messaging to Communicate with Service Users

Document setting out the acceptable use of electronic communication systems and the circumstances in which service users may be contacted using electronic messaging, which includes procedures that must be followed when using these methods of communication

Key Words:	Electronic messaging,	
Version:	1	
Adopted by:	Trust Policy Committee	
Date this version was adopted:	18 February 2020	
Name of Author:	Head of Data Privacy	
Name of responsible Committee:	Data Privacy Committee	
Date issued for publication:	February 2020	
Review date:	July 2022	
Expiry date:	1 February 2023	
Target audience:	All staff including contractors, temporary workers or those on honorary contracts	
Type of Policy	Clinical √	Non Clinical √
Which Relevant CQC Fundamental Standards?	Person centred care; Good Governance; Consent	

**Contents**

**Contents Page ..... 2**

**Version Control ..... 3**

**Equality Statement ..... 3**

**Due Regard ..... 3**

**Definitions that apply to this policy ..... 4**

**THE POLICY**

**1.0 Purpose of the Policy ..... 5**

**2.0 Summary of the Policy ..... 5**

**3.0 Introduction ..... 5**

**4.0 Duties within the Organisation ..... 5**

**5.0 Procedure ..... 6**

**5.1 Advantages ..... 6**

**5.2 Uses ..... 6**

**5.3 Justification ..... 7**

**5.4 Consideration ..... 7**

**5.5 Agreement (Consent) ..... 8**

**5.6 Recording electronic messages in the record ..... 9**

**5.7 Do’s and Don’ts ..... 9**

**6.0 Training Needs ..... 10**

**7.0 Monitoring Compliance and Effectiveness ..... 10**

**8.0 Standards/Performance Indicators ..... 11**

**9.0 References and Bibliography ..... 11**

**REFERENCES AND ASSOCIATED DOCUMENTATION**

**Appendix 1 NHS Constitution Checklist ..... 12**

**Appendix 2 Stakeholder and Consultation ..... 13**

**Appendix 3 Due Regard Screening Template Statement ..... 14**

**Appendix 4 Privacy Impact Assessment Screening Template ..... 16**

**Appendix 5 Guidance Notes Q&A on secure email..... 17**

**Appendix 6 Senders Guide ..... 21**

**Appendix 7 Recipients Guide ..... 22**

**Appendix 8 Standard Operating Procedure template ..... 24**

## Version Control and Summary of Changes

Version number	Date	Comments (description change and amendments)
0.1	25.09.2019	First draft for consultation

### For further information contact:

Head of Data Privacy

Email: [LPT-DataPrivacy@leicspart.nhs.uk](mailto: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 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 3) of this policy.

**Definitions that apply to this Policy**

*All procedural documents should have a definition of terminology to ensure staff clearly understand what is being described (refer to Policy for Policies for assistance).*

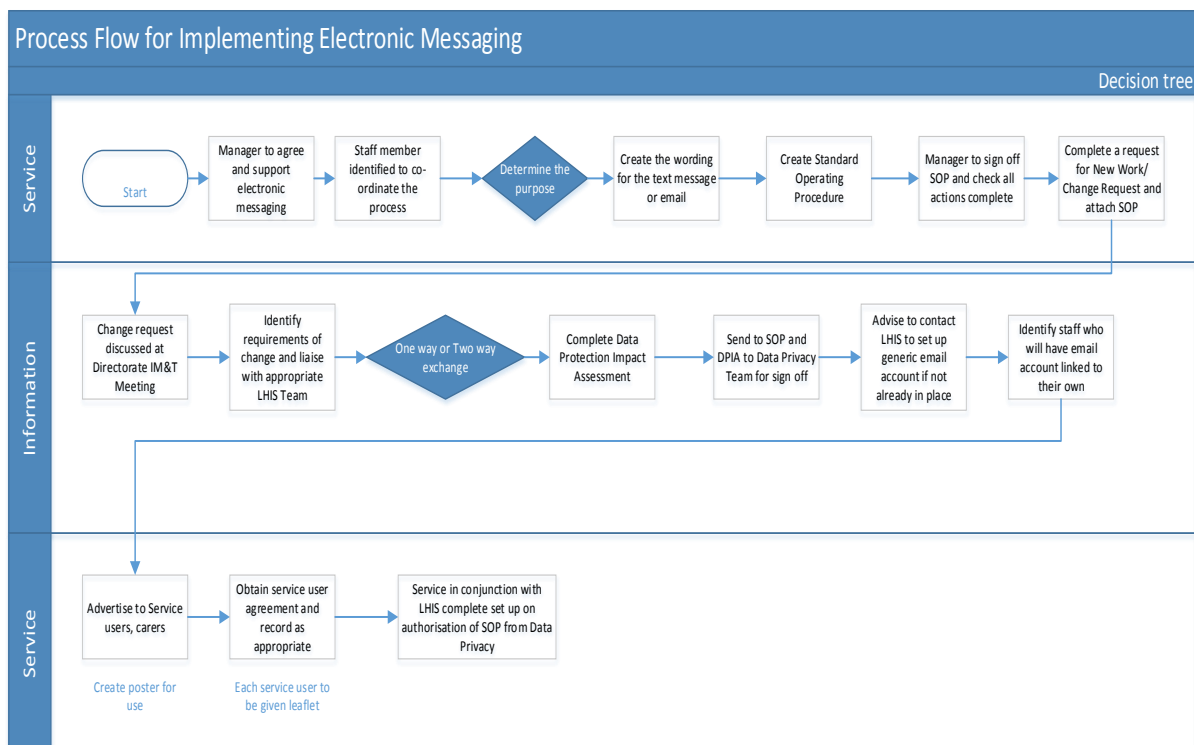
<b>SMS</b>	Short Messaging Service that enables the sending of short messages, commonly known as “text messages” or “texts” to mobile devices
<b>Email</b>	Electronic Mail messages that are distributed by electronic means from one computer user to one or more recipients
<b>Due Regard</b>	Having due regard for advancing equality involves: <ul style="list-style-type: none"><li>• Removing or minimising disadvantages suffered by people due to their protected characteristics.</li><li>• Taking steps to meet the needs of people from protected groups where these are different from the needs of other people.</li><li>• Encouraging people from protected groups to participate in public life or in other activities where their participation is disproportionately low.</li></ul>

## 1.0 Purpose of the Policy

The aim of this policy is to clearly outline the acceptable use of electronic communication systems, which includes but not limited to mobile devices, email and instant messaging. The document also sets out the circumstances in which service users may be contacted using electronic messaging and the procedures that must be followed when using this method of communication.

The principles set out in this policy must be applied by all individuals working for or on behalf of the Trust. This includes contractors, volunteers or third parties in any service that uses electronic messaging to communicate with service users.

## 2.0 Summary and Key Points



## 3.0 Introduction

The acceptable usage of electronic communications, including email and social media, will be specified in order to optimise the benefits of these services to the Trust, whilst protecting the Trust from reputational damage, criticism or litigation, and to ensure that users are able to distinguish official Trust information from the personal opinion of staff.

It is recognised that electronic messaging is a normal part of everyday life and social culture for many of the people that we see within Trust services and it is seen as an opportunity to improve contact, predominantly in relation to appointments.

## 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 Trust Board Sub-committees have the responsibility for ratifying policies and protocols.

- 4.3 Data Privacy Team have the responsibility for supporting the services with their information risk management process relating to electronic messaging with service users
- 4.4 Divisional Directors and Heads of Service are responsible for:  
Ensuring that this Policy is applied and complied within their service when using electronic messaging to communicate with service users
- 4.5 Managers and Team leaders are responsible for:  
Ensuring that this policy is applied and complied within their service when using electronic means of communicating with service users
- 4.6 Responsibility of Staff  
All staff groups must familiarise themselves with this policy and ensure that they follow the principles and processes set out in this document

## **5.0 Procedure**

Staff should not normally use electronic messaging to establish a service users- clinician relationship. Rather, electronic messaging should add to and follow other, more personal contacts, when the service user has given their permission for staff to communicate with them electronically.

Only use electronic messaging with service users who have given their informed agreement for using electronic messaging to communicate with them. This agreement should be clearly documented in their care record.

Even when using secure email or secure file transfer, privacy and confidentiality can be broken, usually as a result of human error. Service users should have the opportunity to accept this risk before staff send any confidential or sensitive information, and this should form part of the agreement discussion.

Use of electronic messaging is not always appropriate, for example when an email relates to mental health treatment diagnoses. Please check with your manager or the Data Privacy team if you are unsure. Any electronic communications with service users must always be saved on the clinical record.

### **5.1 Advantages**

- Speed and ease of use – unlike post, which may take several days to arrive, electronic messaging should be near-instantaneous.
- Reduced postage costs and less impact on the environment
- Likelihood of reduced Did Not Attend (DNA) rates due to the ability to send appointment reminders and quick receipt by the person concerned
- Greater levels of engagement with those services users whose preferred method of communication is electronic

### **5.2 Uses**

Electronic messaging is used primarily for appointment confirmation, reminders and advice/support. However, services in the Trust may use electronic messaging for other purposes which must be approved by inclusion in local standard operating procedures, or, if a one-off exercise, the undertaking and documenting a risk assessment relating to the intended use and having it authorised by the service manager.

The uses of electronic messaging and the service rules governing the contents of messages will vary from one service to another depending on the nature and sensitivity of the service and purpose of the message.

Examples of possible uses of SMS:

- Appointment reminders and confirmations
- Asking the service user to contact the service at a convenient time
- Communicating advice (bad weather reassurance of visit, change in practitioner due to illness)
- Ad-hoc communication between the key worker and service user

Examples of possible uses of Email (Secure):

- Asking the service user to call the service at a convenient time
- Communicating advice (bad weather reassurance of visit, change in practitioner due to illness)
- Ad-hoc communication between key worker and service user
- Appointment letters/Care Plans

Secure File Transfer (WeTransfer) – where service users cannot access via secure email

- Copies of correspondence
- Appointment Letters
- Care Plans

### 5.3 Justification

Services must individually agree the need/benefit of the use of electronic messaging and formally approve and document the implementation of the service in a local Standard Operating Procedure. Individual Trust staff must not use electronic messaging for clinical purposes without formal documented approval.

Local procedures for the use of electronic messaging, which comply with this policy, must be documented and cover the following aspects:

- Identification of the need or justification
- Identification of the service or facility provided i.e. SMS, Email
- How the agreement to use the service by its intended recipients will be obtained
- Clear identification of the associated risks and the means by which these risks will be managed
- How service users will be informed of the availability of the service
- How the service users agreement and preferred method of communication will be recorded

### 5.4 Considerations

Electronic messaging cannot replace letters or face to face contact in communicating important information and should only be used with service users that have agreed or expressed a preference for this form of communication. This agreement and/or preference must be recorded in the service user's clinical record.

Where a service user has expressed a preference to receive email summaries as

opposed to letters, this should be clearly and accurately recorded in their record where it is obvious to all staff who have contact with the. This does not however, negate the requirement to send correspondence to the referrer.

SMS Text messages should only be sent from the Trust issued mobile phone of the appropriate staff member, or the approved system for sending texts. Text messages must only be sent to the phone number provided by the service user or carer to which they have agreed to the Trust using; no other phone numbers should be used.

Emails should only be sent from a generic Leicspart email account for the service e.g. LPT-DataPrivacy@leicspart.nhs.uk. Where relevant, it should be made clear to service users that electronic messaging will not be monitored, and therefore will not be responded to outside of normal working hours.

If a recipient is able to reply to electronic messages, a timescale should be agreed by the service and service users so that if a service user does not receive a response to a message within the agreed time, they can use an alternative method contact such as an appropriate office phone number.

Procedures must be in place for recording the electronic messages into the service user's clinical record and deleting them from phones/email accounts where relevant.

A service Standard Operating Procedure must be written and agreed by the Data Privacy Team and a Data Protection Impact Assessment (risk assessment in relation to the information flow) completed with the Data Privacy Teams assistance.

## 5.5 Agreement (consent)

Prior to sending any electronic messages to any service user, their informed agreement must be obtained explaining all the appropriate information to them. Their verbal agreement is acceptable for routine uses such as appointment reminders, asking the service user to call the service or communicating advice. Written agreement must be obtained for using Trust issued mobile phones and email accounts for conversational messaging with service users and carers. For any other purpose not included in section 6.2, the Data Privacy Team must be consulted.

The use of service users mobile phone numbers if provided for these purposes, is outlined in the Trust Privacy Notice.

Service user's agreement must be recorded in the specific place for consent recording in the service user's record in their electronic health record. Service users must be made aware that they can opt out of the electronic messaging service at any time in the future.

When asking for their agreement to electronic messaging, service users must be made aware of their responsibility to keep the services they use, up to date with their correct number and/or email address that they wish to be contacted on.

Service users should be made aware of all options for communication (phone, letter, text, email etc.) and their preferences recorded on the electronic health record. It should also be made clear to the recipient that any correspondence will be added to their record.



Where a service user/carer has asked (and subsequently agreed) to be communicated with via email it is advised that the service user is asked to email their request to the relevant service generic email address to verify their email address before any correspondence takes place. A copy of this email should be placed on the service user's record and any correspondence must be sent encrypted using the secure email instructions found at Appendix 5.

#### 5.6 Recording electronic messages in the record

Any electronic communication about a service user either between clinicians/practitioners/admin support staff, or the service user themselves, and/or their carer must be recorded in the service user's clinical record. This includes:

- Electronic conversations regarding the delivery of care, details of any appointments, or changes to appointments
- Electronic conversations regarding the service user with other agencies/individuals involved in the delivery of care
- Electronic communications from carers, or other significant people involved in the care of the service user
- Electronic communications from clinicians/practitioners/admin support staff to and from the service user.

For email communications the clinically relevant content of the email must be copied and pasted into the record. Copied information must include the date and time of the original email(s), sender and recipients email(s), as well as the date/time entered into the electronic record.

For text conversations, these should be transcribed into the service users record including the date and time it was sent and received and the phone number it was sent to/from.

It is the responsibility of each clinician/practitioner/admin support staff to review the content of the email trail to ensure:

- Only clinically relevant information is copied into the service users record;
- All 3<sup>rd</sup> party information (that is not relevant to the service user and/or their care) is removed before the content of the email is copied into the service users record;
- Each clinician/practitioner/admin support staff is responsible for ensuring that the right information gets into the right service users record;
- Once the clinician/practitioner/admin support staff has ensured that the service user's record is up to date and accurate, the emails should be deleted from the email inbox.

#### 5.7 Do's and Don'ts

##### DO

- Make service users aware that electronic messages must not, under any circumstances, be used in emergency situations and should be advised of the correct method(s) of contacting emergency services
- Keep electronic messages formal and maintain professional standards. Avoid giving personal comments or opinions
- Ensure texts are written in full without using "text speak" or abbreviations

- Ask the service user to clarify any abbreviations or “text speak” they have used in an electronic message – make no assumptions
- Always respond to messages within an agreed timescale where relevant
- Only send electronic messages within normal working hours
- Only used a Trust issued mobile phone for sending text messages to service users – no other phone should be used
- Only use an email address belonging to the Trust to send emails and these should be encrypted – no other email addresses should be used
- In case an electronic message is seen by someone other than the intended recipient, avoid using unnecessary identifiers of the service user or service

## DO NOT

- Do not use inappropriate language in electronic messages that could cause offence, such as swearing or racial comments. If you receive any such messages it should be reported via the Ulysses system (e-IRF) and fully detailed, with a verbatim transcription in the service users record
- Do not use predictive text as this can cause unintended modifications and change or confuse the meaning of the message
- Never use electronic messages to convey personal or sensitive information
- Do not use instant messaging such as Facebook messenger, WhatsApp, with service users

## 6.0 Training needs

There is no training requirement identified within this policy but the following staff will need to be familiar with its contents:

All personnel (including staff, contractors, volunteers and third parties) in any service that uses electronic messaging to communicate with service users.

As a Trust policy, all staff need to be aware of the key points that the policy covers. Staff can be made aware through Team Brief, e-Newsletter and team meetings.

## 7.0 Monitoring Compliance and Effectiveness - complete the template below

Ref	Minimum Requirements	Evidence for Self-assessment	Process for Monitoring	Responsible Individual / Group	Frequency of monitoring
8	SOPs are created for each Service wanting to offer e-Messaging	Section 5.3 & 5.4	SOPs approved	Data Privacy Team	Ad-hoc
9	Electronic messages are accurately recorded in the service user record	Section 5.6	Local record keeping monitoring	Clinical Supervisors	Ad-hoc
8	An agreement is in place with the	Section 5.5	Local record keeping monitoring	Local record keeping monitoring	Ad-hoc

Ref	Minimum Requirements	Evidence for Self-assessment	Process for Monitoring	Responsible Individual / Group	Frequency of monitoring
	service user				

## 8.0 Standards/Performance Indicators

This policy supports the following CQC Fundamental standards:

- Person-centred care – through acting on service users communication preferences
- Consent – There is an agreement in place with the service user in relation to the method of communication
- Good governance – the Standard Operating Procedures and approval process represent the measures taken to ensure risks are managed

## 9.0 References and Bibliography

The policy was drafted with reference to the following:

- Record Keeping and Care Planning Policy May 2018
- Information Risk Policy February 2018
- Data Protection Impact Policy and Procedure October 2019

## 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

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

## Appendix 2

### Stakeholders and Consultation

#### Key individuals involved in developing the document

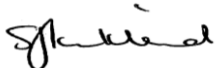
Name	Designation
Chris Biddle	Cyber Security Manager
Graham Calvert	FYPC Clinical Lead for IT and Information Governance

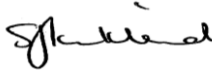
#### Circulated to the following individuals for comment

Name	Designation
Members of IM&T Delivery Group	
Members of Data Privacy Committee	

## Appendix 3

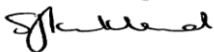
### Due Regard Screening Template

Section 1			
<b>Name of activity/proposal</b>		Electronic Messaging with Service Users Policy	
<b>Date Screening commenced</b>		25 September 2019	
<b>Directorate / Service carrying out the assessment</b>		Enabling/Data Privacy	
<b>Name and role of person undertaking this Due Regard (Equality Analysis)</b>		Head of Data Privacy	
<b>Give an overview of the aims, objectives and purpose of the proposal:</b>			
<b>AIMS:</b> To meet the communication needs of service users whose predominant means of communication is electronic			
<b>OBJECTIVES:</b> To ensure that electronic communications with service users are conducted in secure and robust parameters			
Section 2			
Protected Characteristic	If the proposal/s have a positive or negative impact please give brief details		
Age	No impact		
Disability	Positive – the Trust can securely cater to their communication needs		
Gender reassignment	No impact		
Marriage & Civil Partnership	No impact		
Pregnancy & Maternity	No impact		
Race	No impact		
Religion and Belief	No impact		
Sex	No impact		
Sexual Orientation	No impact		
Other equality groups?			
Section 3			
<b>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 <u>tick</u> appropriate box below.</b>			
Yes		No	
High risk: Complete a full EIA starting click <a href="#">here</a> to proceed to Part B		Low risk: Go to Section 4.	✓
Section 4			
<b>If this proposal is low risk please give evidence or justification for how you reached this decision:</b>			
This option of communication is available for all service users and supports the embedding of the Accessible Information Standard in order to meet the communication and information needs.			
<b>Signed by reviewer/assessor</b>		<b>Date</b>	20/01/20

<i>Sign off that this proposal is low risk and does not require a full Equality Analysis</i>			
<b>Head of Service Signed</b>		<b>Date</b>	20/01/20

## Appendix 4

### DATA PRIVACY IMPACT ASSESSMENT SCREENING

<p><b>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.</b></p> <p><b>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.</b></p>		
<b>Name of Document:</b>	<b>Electronic Messaging with Service Users</b>	
<b>Completed by:</b>	<b>Sam Kirkland</b>	
<b>Job title</b>	<b>Head of Data Privacy</b>	<b>Date: 25/09/2019</b>
<b>Screening Questions</b>	<b>Yes / No</b>	<b>Explanatory Note</b>
<b>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.</b>	No	
<b>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.</b>	Yes	If the service users wants to be communicated with electronically they will need to provide a mobile phone number and email address
<b>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?</b>	No	
<b>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?</b>	No	
<b>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.</b>	Yes	Text messaging and emailing within tight parameters
<b>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?</b>	No	
<b>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.</b>	No	
<b>8. Will the process require you to contact individuals in ways which they may find intrusive?</b>	<b>No</b>	
<p><b>If the answer to any of these questions is 'Yes' please contact the Data Privacy Team via <a href="mailto:Lpt-dataprivacy@leicspart.secure.nhs.uk">Lpt-dataprivacy@leicspart.secure.nhs.uk</a></b></p> <p><b>In this case, adoption of a procedural document will not take place until review by the Head of Data Privacy.</b></p>		
<b>Data Privacy approval name:</b>	<b>Sam Kirkland, Head of Data Privacy</b> 	
<b>Date of approval</b>	<b>20/01/20</b>	



## Appendix 5

# Guidance Notes - Questions and Answers

## *Secure e-mail for Personal Confidential Data (PCD)*

### **What is the current Policy?**

---

Policy permits the secure transmission of business sensitive information by email, and also permits, the secure transmission of Personal Confidential Data (PCD) by email in defined circumstances: -

1. Communication about individuals shared within the NHS networks to those with the need to know
2. Communications to external involved parties (e.g. those covered by third party sharing agreements) such as Social Care, the Police, the Coroner
3. Case by case with solicitors, advocates, nursing homes, and investigators
4. Business communications concerning claims and complaints (e.g. CQC, Parliamentary Ombudsmen)
5. Direct e-Communications with Patients – Policy requires that Services permitting e-communications with patients must have a service specific patient communications policy for the guidance of their staff.

Any other requirement to share PCD should first be raised with the Information Governance Lead for your organisation.

### **What is Personal Confidential Data?**

“Personal identifiable data” is data which relates to a living individual who can be identified from the data, or by matching that data to other data in the possession of a data controller.

However ‘Personal confidential data’ is different as it includes a range of information including physical or mental health conditions, political or religious beliefs, racial or ethnic origin, or sexual life.

Within the NHS, the phrase may be applied to patient related or to staff related information. Under the Access to Health Records Act, there is also a duty to safeguard the confidentiality of deceased patients.

### **What can I do now?**

If your job role permits you to send PCD as defined above, you may send using the local email system. Any email containing PCD in the body of the email or in an attachment must be secured.

In order for the email to be secured, the sender must insert square brackets around the word secure into the subject line of the email:- [secure]

Emails which do not contain PCD or other business sensitive information should not be labelled as [secure].

## **How secure is email sent via [secure] in the subject line?**

The [secure] identifier enables the email to be appropriately directed via secure routes, or encrypted, before it is directed to the recipient.

This uses a LHM maintained master list of securely connected email systems. Those email addresses not on this list require the email to be encrypted.

A message will be automatically generated, where appropriate, to advise the recipient that the email has been sent to them, by an NHS approved secure route.

Instructions on how to access, and how to respond to the email, should be sent to those recipients who are outside our secure or securely linked networks (e.g. solicitors, advocates, patients). This will familiarise them with what to expect.

## **The sender must send to a correct address**

Be aware that when using [secure], it is a sender responsibility to correctly address the email. A misaddressed email can be opened by its unauthorised recipient.

Both recipient and sender must manage their accounts to minimise the amount of patient information stored within them.

As is usual with technology, we, the users, are the weakest link in the chain.

## **What can/can't I send?**

### ***When sending [secure] emails***

PCD information should not appear in the subject line of the email.

Email best practice is to send long correspondence in an attached document. (This does not prohibit sending of sensitive information within the email body)

## **What are the risks of sending PCD using [secure], and how can I reduce them?**

### ***Breach of patient confidentiality***

- The sender must ensure that the email is addressed correctly. Send a test email (not addressed as [secure]) to be sure or reply, to a previous email known to be the correct email address. If you are sending a test email, this is an ideal opportunity to send the recipient guidance so they fully understand the process before they receive your encrypted email
- When forwarding [secure] PCD, [secure] will be inserted into the subject line of the forwarded email
- Do not email groups unless it is relevant to all members

- Do not set auto-forwarding on your email account. Sensitive messages received must terminate securely at your local work email address
- The recipient must understand the confidential nature of the data
- State that the information is confidential
- To avoid including your source data in error, use PDF format if you have embedded charts or tables in reports
- State that data received in error should be deleted, and the named contact or sender informed
- Follow a Clear Desk Clear Screen Policy and ensure that you are not overlooked.
- Ensure that data received is stored in the appropriate permanent record e.g. the patient record, or complaint file
- Do not store PCD in email systems. Move email and attachments to a safe area and delete patient data held in your inbox, sent items or other email folders
- On receipt of a misaddressed email, inform the sender and delete it from your inbox and from the deleted items mailbox.

### ***Clinical Risk/ Maintaining the Patient Record***

- Ensure the recipient regularly checks their email
- If you are emailing an individual ensure the recipient has sole access to their email account
- Ensure that you both have alternative means of contacting each other e.g. phone. So you can speak the recipient and ensure the safe transit of your email
- Include your contact details when you send
- Do not rely upon secure email to pass on referrals or clinical responsibility without appropriate follow up; the recipient may be absent. Ask for a confirmation email
- Do not replace usual clinical documents by longwinded emails; your structured template will be easier to understand and can be attached.

### ***Failure to maintain expected professional standards***

When emailing patient information you must keep messages considered, professional, polite and to the point (do not mix personal messages in any email or attachments which may become part of the patient/client record).

### **What do I do if a breach has occurred?**

If there is a breach of confidentiality or a clinical risk is identified, call the LHM Service Desk (0116 295) 3500, and report the incident via an e-eIRF (the organisation incident management reporting process).

### **Remember**

- Report loss of hand held equipment (e.g. Smartphones/ tablets) which hold work email; remember the LHM can remotely lock and wipe these devices. Do not delay
- If a message is sent to the wrong address, a recall is unlikely to work. You should send a follow up message asking the recipient to delete the previous message and report the breach to the Service Desk and to your IG lead.

**Who do I contact for clarification or further information?**

LHIS Service Desk, (0116 295) 3500

Ref: Procedures for sending and for the receipt of [secure] PCD or of business sensitive information.

## Appendix 6

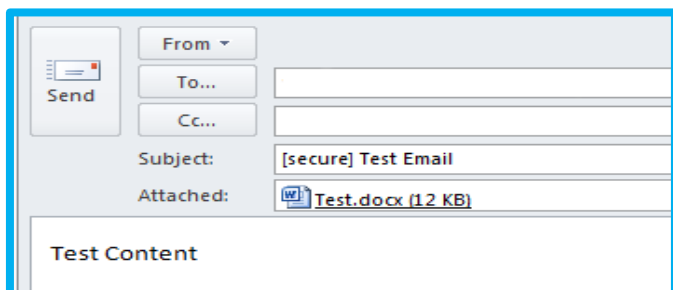
# Secure email: Sender's Guide

## Sending a secure email

1. Notify the recipient **by normal email** of your intention to send information by secure email and attach a copy of the 'SecureEmailRecipientsGuidev2', which explains how to register for an account to receive the information. **DO NOT send any personal information with this email.**

NOTE: If you are sending an email using the secure email solution to a recipient at Leicester City Council, Leicestershire County Council, UHL, or LPT you do not need to send a recipients guide, their email is already secure and they will not need to register.

2. Open a new email in Outlook
3. Type [secure] in the subject line of the email, i.e. the word secure in \*square brackets, followed by your own subject title for the email.



4. Complete the email in the normal way, including any attachments. **Remember:** As the sender, you **must** be assured that you are using the correct email address.
5. Send the email.

**The confidential information has now been sent to the recipient by secure email.**

To retrieve the information the recipient will need to register an account. Once an account has been registered, they will not need to register again (unless their password has been inactive for 180 days) and any further secure emails will require only their account password to open.

\*If you're not familiar with the square brackets they are located on the keyboard as per the below:



## Appendix 7

# Secure email: Recipient's Guide

In order to view a secure email from NHS senders in Leicestershire, you will need to register with the secure email portal. To access the message you will need Acrobat Adobe version 7.0 or higher.

Please follow the guidance below to create your account. Once you have registered a password with the portal, you will be able to use this same password to view this, and future secure emails sent by anyone in the Leicestershire Partnership NHS Trust, CCGs and General Practice.

If your password is not used to access a secure email for 10 days, your account will be deleted. If you are sent another email after your account is removed, you will simply have to follow this process again to create a new account.

## Receiving a secure email message and opening an attachment

1. You will receive a notification email to advise you that there is a secure email waiting for you:
2. Click [here](#) in the email to access the secure email portal (If you have already registered with the portal you will be directed straight to point 4)
3. You will be asked to create your account. Please make sure you use a memorable, strong password.
4. Once you have registered you will be sent an email with the message as an **attached PDF document**.



**To open the attachment:** you will need to save the document to your device

5. Click on the PDF document to open the email message sent to you; you will be prompted to enter your account password. Your message will appear on Page 2. **NOTE: To view any attachment sent with your message, you will need to save the document to your device:**
  - Right click on the message and select 'Save As'.
  - Save the document to your device.

- Open the document on your device with your account password.
- Any attachment(s) will now be available at the bottom left of the screen under the following banner:

Name ▲	Description	Modified	Size	Compressed size
--------	-------------	----------	------	-----------------

6. If you are unable to access the message contact the original sender to make alternative arrangements.

*PLEASE NOTE: Secure email may contain personal information. The sender takes no responsibility for its onward disclosure by the intended recipient.*

## How to reply to a secure email

In order to reply to a secure email **you will need to click 'Reply' from within the secure message.**

Scroll down to the Page 2 of the message to see the reply button:



Write your response as you would a normal email, and click 'Send'.

## Appendix 8



**Leicestershire Partnership**  
NHS Trust

**INSERT TITLE OF SOP**

For Completion by SOP Author	
Version	Insert [Draft Version & Number] Please also Amend Footers. <i>[Draft version will be changed to Issued Version by the SOP Controller on approval]</i>
Document Author(s)	Insert Author(s) and Job Title(s)
Document Reviewer(s)	Insert Document Reviewer (s) and Job Titles(s)

For Completion by Author	
Name of Responsible Committee	Research Quality Committee, [Insert Date Ratified]
Issue Date	Insert Date Issued <i>(Change Version, Footers &amp; Watermark)</i>
Implementation Date	Insert Agreed Date for Implementation)
Review date	Insert Agreed Review Date



## CONTENTS

1. INTRODUCTION.....	
2. SCOPE .....	
3. ABBREVIATIONS & DEFINITIONS.....	
4. DUTIES AND RESPONSIBILITIES.....	
5. PROCESS .....	
6. TRAINING REQUIREMENTS .....	
7. REFERENCES AND ASSOCIATED DOCUMENTATION .....	
8. VERSION HISTORY LOG.....	
Version.....	
9. APPENDICES.....	

### 1. INTRODUCTION

Insert a brief introduction to the SOP. This may include a background summary and reference any legislation, standards or guidance which may have lead to its development.

### 2. SCOPE

Describe one or more of the following:

- Who the SOP applies to (which staff members)
- The sorts of activity the SOP applies to

### 3. ABBREVIATIONS & DEFINITIONS

Insert the meaning of any commonly used abbreviations (e.g. SOP = Standard Operating Procedure) and definitions.

### 4. DUTIES AND RESPONSIBILITIES

Summarise the duties and responsibilities of key staff involved in conforming to the SOP

### 5. PROCESS

Describe the procedure(s) to be followed. Wherever possible use a numbered list which can be followed step-by-step, or consider using a flowchart for more complicated procedures. In some cases it may be appropriate to have more than one procedure in which case you should create a new section for each procedure. Language should be clear and instructive

**Please refer to the Electronic Messaging with Service Users Policy for points for consideration**

#### 5.1 Type of Messaging to be used

SMS Text – One way or Two way, purpose of the message frequency and system to be used  
e.g. NHS Mail, Trust mobile

Email – sending address and validation of recipient address

#### 5.2 Managing the messaging system

Admin support

Team responsibilities

Monitoring messages

Check for failed messages

How staff will be supported to use the system and kept up to date

### 5.3 How agreement (consent) will be obtained

Type of agreement (consent) required (please refer to the policy), use of leaflets, discussion with service user/carer, obtaining and maintaining correct mobile phone numbers/email addresses, their responsibilities, recording agreement in the clinical record, maintaining their agreement status e.g. if a service user changes their mind

### 5.4 How electronic SMS and Email service will be marketed

Posters

Leaflets

Discussion with service users

Service information on website

## 6. TRAINING REQUIREMENTS

Describe:

- Who is required to be trained in the SOP
- Who is going to provide the training and frequency of this training
- Specify if evidence of training in the SOP should be checked/verified at study initiation

Insert the following standard text for Trust-wide SOPs:

- When a new SOP is authorised, or when an existing SOP is revised staff should take time to read and fully understand the SOP and relevant documents, ensuring that they are able to implement the SOP when required. If clarification is needed then staff should approach their line manager who will decide if additional training is required and that the training is documented in their training record.

## 7. REFERENCES AND ASSOCIATED DOCUMENTATION

Reference:

- Other related policies & procedures
- Texts or key documents referenced in the body of the SOP

## 8. VERSION HISTORY LOG

This area should detail the version history for this document. It should detail the key elements of the changes to the versions.

Version	Date Implemented	Details of Significant Changes

## 9. APPENDICES

Insert each appendix as a new section, including

**Signatures for relevant staff to sign**

I confirm that I have read and consider myself to be sufficiently trained in the above Standard Operating Procedure with regards to my individual roles and responsibilities

Signature of Trainee ..... Date  
.....

I confirm training in the above SOP was delivered as recorded above and that the trainee may be considered sufficiently trained in their roles and responsibilities

Signature of Trainer ..... Date  
.....

**Additional Notes & Signatures**

Signature of Trainer (where appropriate)

I confirm training in the above SOP was delivered as recorded above and that the trainee may be considered sufficiently trained in their roles and responsibilities

Signature of Trainer ..... Date  
.....