South Eastern Health and Social Care Trust

Policy Code: SET/Gen (107) 2014

SOUTH EASTERN TRUST

Title:	**Transferring Personal Information Policy & Procedures**		
Authors(s):	**Information Governance Manager**		
Ownership:	**South Eastern Health & Social Care Trust**		
Approval by:	**Ratified Directors as per signatory list**	**Approval Date:**	**February 2013**
Operational Date:	**February 2015**	**Next Review:**	**February 2017**
Version No:	**2.0**	**Supercedes:**	**SET/Gen (35) 2011**
Key Words:	**Transferring/Personal/Information**		
Links to Other Policies:	**Data Protection Policy** **Freedom of Information Policy** **Records Management Policy Statement** **Records Management Procedure** **Email Encryption User Guide for 3rd Party Recipients** **Policy on Email Management**		

1.0 INTRODUCTION / PURPOSE OF POLICY

1.1 In accordance with the Data Protection Act 1998, all staff working for, or on behalf of the South Eastern Health & Social Care Trust (the Trust) must ensure that personal information is only made available to those who have been authorised to receive it.

Every effort must be made to ensure that any information being shared/transferred electronically or manually is done so securely.

1.2 Transferring personal information may be on an individual basis or as a bulk transfer. Examples of information transfers include:-

- Where internal post is used to send correspondence about a patient;
- Transfer of a service user record by a member of staff;
- 20 service user records sent in one envelope from one Trust location to another, by internal post, external post or courier;
- Several hundred electronic records sent via email to an non- Health & Social Care (HSC) organisation;

- 50 electronic staff records copied onto removable media and taken out of the building to another location e.g. to be uploaded to a computer there.

1.3 Sending personal information by any communication method has security risks attached to it. This can lead to a breach in confidentiality and risk to service use care.

1.4 It is essential to minimise these risks as much as possible while still meeting business needs. When transferring personal information it is essential to establish safe working practices to protect its security and confidentiality.

2.0 SCOPE OF POLICY

2.1 Compliance to this policy is mandatory for all staff both permanent and non-permanent and for whom the Trust has legal responsibility. The Line Manager must ensure compliance within their respective areas of control and responsibility.

2.2 This policy supports staff in implementing national and local best practice and legislative requirements on the transfer of personal information.

3.0 ROLES AND RESPONSIBLITIES

3.1 All Staff

All staff have responsibility to be aware of and to adhere to this policy:-

- Adhere to this policy when transferring personal information;
- Bring to managers attention areas of concern regarding transfer of personal information;
- Seek advice from the Information Governance (IG) Team and or ICT Security Team (Contact details at end of this document) when unsure about the most appropriate methods of transferring personal information.

3.2 Data Guardians (Medical Director and Director of Children's Services & Executive Director of Social Work)

The Data Guardians are supported by the ICT, Risk Management & Governance Teams and have a responsibility to:-

- Safeguard and govern uses made of personal information within the Trust, as well as data flows to other Health & Social Care (HSC) and non-HSC organisations;
- Oversee the establishment of procedures governing access to, and the use of, person identifiable and, where appropriate, the transfer of that information to other organisations;

- Ensure that Data Access Agreements (DAA) are in place for all routine transfers of information outside the Trust, in accordance with DHSSPS guidance.

3.3 Senior Information Risk Owner (SIRO)

The Director of Human Resources & Corporate Affairs fulfils the role of the Trust's SIRO and is responsible for the management of information risk at Board level. The role of the SIRO is to lead and foster a culture that values, protects and uses information for the public good. He/she will advise the Accounting Officer (Chief Executive) on the information risk aspect for the Trust's Statement of Internal Control. The Director for Planning, Information and Performance Management acts as the Deputy SIRO.

3.4 Information Asset Owner (IAO)

The Trust's Assistant Directors fulfil the role of IAO. He/she will have a full understanding of their Directorates information assets, and who has access to this information.

3.5 Line Managers

Line Managers have a responsibility to:-

- Ensure that this policy is brought to the attention of all staff;
- Ensure all current, new and temporary staff are instructed in their responsibilities in relation to transfer of personal information and work in accordance with this policy;
- Investigate and take relevant action on any potential breaches of this policy supported by risk management leads and the IG Team in line with existing procedures;
- In certain circumstances support Equality and Diversity by considering the individual requirements of staff in order to support them in complying with this policy.

3.6 Information Communication & Technology

ICT has a responsibility to:-

- Provide further advice and guidance to staff when required;
- Implement security processes to protect personal information transferred electronically.

3.7 Information Governance Team and related Information Governance Structure

The IG Team and related IG Structure have a responsibility to:-

- Develop and support the implementation of the Transfer of Personal Information Policy and Procedures and ensure the Trust meets legislative requirements;

- Ensure that the Trust meets its transfer of personal information obligations as specified in the Information Management & ICT Controls Assurance Standards.

4.0 KEY POLICY PRINCIPLES

4.1 Definitions

4.1.1 Personal Information

This is also referred to as, “person-identifiable information (PID)” and relates to information about a person which would enable that person’s identity to be established by one means or another. This might be fairly explicit such as an unusual surname or isolated postcode or bits of different information which if taken together would allow the person to be identified. All information that relates to an attribute of an individual should be considered as potentially capable of identifying them to a greater or lesser extent.

PID data can relate to information held about any individual, not just service users. It may, therefore, include information about staff, contractors, visitors and members of the public.

4.1.2 Sensitive Personal Information

This is information where loss, misdirection or loss of integrity could impact adversely on individuals, the Trust or on the wider community, eg;

- Health or physical condition;
- Sexual orientation;
- Ethnic origin;
- Religious beliefs;
- Political views; or
- Criminal convictions.

In addition to personal information and clinical information, financial and security information is also likely to be deemed “sensitive”.

For sensitive personal information even more stringent measures should be employed to ensure that the data remains secure.

4.1.3 Approved Courier

Approved courier is a courier selected from a contracted or authorised list, as agreed by the Trust.

4.1.4 Bulk Transfer

Bulk transfer is defined as the transfer of electronic or paper data that is "batched up" to be sent out of a location and/or organisation.

4.1.5 Consent

Consent is an agreement to an action based on knowledge of what the action involves and its likely consequences.

4.1.6 Data Access Agreements (DDA)

DDAs set out the basis for the secure transfer and use of personal data across both HSC and non-HSC organisations.

4.1.7 Encryption

Encryption is the process of converting information into a form unintelligible to anyone except holders of a specific key or password.

4.1.8 Removable Media

Removable media is a term used to describe any kind of portable data storage device that can be connected to and removed from a computer e.g. floppy discs, CDs/DVDs, Trust ironkey (memory stick), PDAs. For further detail on different types of removable media see the Information Communication & Technology (ICT) Security Policy.

4.1.9 Safe Haven

A safe haven is a location which is set up to receive and manage confidential information appropriately. It may be a post room or fax machine, or anywhere were personal information may be taken and held securely before being passed onto the appropriate recipient.

4.1.10 Honest Broker Service

This service is available via Business Services Organisation (BSO) and does not include the transfer of personal data.

4.2 POLICY PRINCIPLES

4.2.1 Risks In Transferring Personal Information

4.2.2 There are a number of risks associated with transferring personal information. Without adequate security processes to protect personal information in transit there will always be risks to that information. The severity and type of these risks will vary depending on the method of transfer. Examples of such risks include:-

- Information being lost, damaged or intercepted in transit e.g. stolen laptops, mobile phones, opened envelopes;

- Delivery service delivering mail incorrectly;
- Information being sent to the wrong address via e-mail, post or fax;
- Information received by the organisation but not delivered to the correct person;
- Confidential conversations being overheard; and
- Personal information not being disposed of appropriately.

4.2.3 Where such risks are realised and personal information is compromised there is an impact on the following:-

- Individuals – whose information has been put at risk;
- Staff – whose actions placed the information at risk
  - Such staff may have breached local policy and this could potentially lead to disciplinary action. There may also be legal implications if they have breached information legislation.
- Organisations – whose actions placed the information at risk
  - Such organisations may experience a lack of trust or confidence from the public and potential prosecution under information legislation.

4.2.4 All risks and incidents relating to the transfer of personal information must be reported using the Trust's Incident Reporting procedure (IR1). The Trust's policies on incident reporting provide further guidance on this process which can be found on the Trust's intranet.

4.2.5 Reporting of risks and incidents is important to ensure that appropriate action is taken so that risks/incidents do not reoccur and to learn from them. No constructive action can be taken if the Trust is not notified when things go wrong or there is a near miss.

4.3 Transfer of Personal Information (Appendix 1)

4.3.1 <u>Good Practice Principles when Transferring Personal Information</u>

Before transferring any personal information the following "Caldicott" Principles should be applied:-

- Justify the purpose for which the information is required;
- Only use personal information when absolutely necessary;
- Use the minimum personal information possible;
- Access to the information should be on a strict need to know basis;
- Everyone should be aware of their responsibilities to respect the confidentiality of personal information;
- Understand and comply with the law.

4.4 Requirements for Transferring Personal Information

4.4.1 Adequate security processes are essential to protect personal information during transfer. It is appropriate to use different methods of transferring personal information for different circumstances. Careful consideration must be given to the most appropriate method based on the purpose, format, whether individual or bulk transfer and inherent risks involved.

4.4.2 This section defines the different methods of minimising the risks when transferring personal information in different way and provides information on individual and bulk transfers.

4.5 Bulk Transfers

4.5.1 It is essential that all services have in place systems to ensure that bulk transfer of personal information are appropriately controlled, implementing appropriate security measures around such transfers.

4.5.2 All new bulk transfers must be authorised by Assistant Directors/IAO. They will decide whether to authorise the transfer of this information after careful consideration of content, format and method of transfer. It will be their responsibility to ensure that the IG team / Information & Systems (ICT) is informed, and that a Data Sharing Agreement is set up.

4.5.3 A log will be held by the Information & Systems Team of all routine and ad-hoc transfers of bulk personal information (based on information flow reviews) and this will be updated as Information & Systems is informed of new transfers.

4.6 Email (Appendix 1)

4.6.1 Personal information sent by email should be encrypted unless it is being sent from one individual to another on the same network, or when networks are connected via a secure link as in the case of HSC organisations.

4.6.2 There are a variety of ways of encrypting emails, one being sending the information from one HSC mail account (i.e. email address ending in hscni.net) to another, where encryption is done automatically when a message is sent.

4.6.3 If information cannot be transferred via HSC mail, then other encryption methods should be used. Further guidance can be obtained by contacting the ICT helpdesk.

4.6.4 In rare circumstances, the above forms of securing information may not be possible but information may need to be communicated by email to meet business needs, i.e. communication with non-HSC providers. In such circumstances specific agreement must be received from the

Data Guardian for this type of information to be shared and the method used.

4.6.5 The ICT department will continue to look at improved methods of securing email communication, reviewing current and emerging technologies in line with national and local guidance.

4.6.6 Even when the above conditions are met, the following points need to be adhered to:-

- Ensure that the name and email address of the recipient are correct;
- Ensure a suitable subject heading is used i.e. not including personal information;
- Ensure email is clearly marked confidential and the information provided is minimal;
- Ensure the recipient is expecting the information so that it can be acted on without delay;
- Ensure the message has been received;
- Ensure that the information within the email is stored in the agreed format;
- Ensure one email is sent per service user if email contains information to be filed in the service user record.

4.6.7 If consideration is being given by service areas to communicate with service users via email, it is essential to seek guidance on any potential security and confidentiality implications from the IG and ICT teams and have this agreed with the IAO.

4.7 External & Internal Post/Courier (Appendix 2)

4.7.1 Postal and courier services can be used to transfer personal information either in paper format or as electronic information on removable media.

4.7.2 There are a number of standard requirements which must be adhered to when transferring information by post or courier services. There are also additional requirements around removable media and bulk transfers. Refer to Section 6.3.2.3 for further guidance.

4.7.2.1 <u>Standard Requirements</u>

- Confirm the name, department and address of recipient and enter details correctly on the envelope/parcel;
- Mark the envelope/parcel, private and confidential and add on return address details where this will not compromise confidentiality;
- Package securely to protect the contents from being tampered with or from any physical damage likely to arise during transit e.g. a tamperproof wallet;

- Consider use of an approved courier or secure mail method which can be tracked and is signed for e.g. Royal Mail Special Delivery/Recorded delivery;

4.7.2.2 Media Devices

Due to the level of security required in transfer of patient identifiable or sensitive information, the Trust will not allow the use of media devices for the transfer of personal data unless authorised by the IAO and the ICT Manager. The following devices should not be used until authorisation is given:

- USB Data storage;
- CD/DVD; and
- Floppy Disk.

Personal identifiable information loaded to the above must be encrypted to HSC guidelines (seek advice from ICT Manager). The use of freeware or shareware that does not benefit from independent security evaluation or that fails to comply with these standards is not permitted and must be avoided.

Where permission to use a removable media device is given the following guidance should be adhered to:-

- Electronic personal information to be sent by post or courier, must be encrypted prior to transfer, in line with the ICT Security Policy;
- Processes must be in place for the appropriate disposal of information on the removable media once transfer is complete.

4.7.2.3 Bulk Transfers

- When transferring bulk personal information you must use an approved courier or secure mail method which can be tracked and is signed for e.g. Royal Mail Special/Recorded Delivery;
- When transferring personal information by approved courier:
  - The individual responsible for passing the information to the courier, must check the ID of the Courier and obtain a receipt from the Courier when the bulk personal information is collected;
  - The sender should confirm the bulk transfer has been received;
  - The courier must only hand this information over to the recipient or to a nominated individual and obtain a signature when delivered.

4.8 In Person

4.8.1 On occasions, personal information may need to be transferred in person. This may be due to the needs of the service or because this may be the most secure method of transferring the information. Examples of this include handling a service user record over to a colleague off site, handing over an encrypted CD or personal data to another organisation etc.

4.8..2 Due to the number of different approaches to transferring personal information in person e.g. on foot, by car, public transport, in electronic or paper formats, it is not possible to give a definitive list of actions to be taken. However, careful consideration must be given to all the potential security and confidentiality risks involved and agree and document actions to mitigate these.

4.9 Telephone (Voice) – (Appendix 3)

4.9.1 Using telephone voice facilities to transfer personal information may include the following – discussing cases with colleagues, speaking directly with service users, booking appointments. Any discussion involving personal information may have confidentiality implications and as such will be covered by the DHSSPS Code of Confidentiality on Protecting Service User Information. However, if this information is recorded in some way e.g. notes taken from a telephone conversation, messages on answer phone, then the following key points should be adhered to:-

1. Services should only use answer phones for leaving personal information after careful consideration of the security and confidentiality risks involved;
2. Ensure answer phone messages cannot be overheard when be played back, consideration should be given to a safe haven answer phone;
3. The answer phone should be protected by pin number access or in a locked room when unattended to prevent unauthorised access;
4. Personal information should only be given over the telephone to the intended recipient or their agreed representative;
5. The person making the call should always check whether it is convenient for the recipient to receive the information before passing it on;
6. The intended recipient should be asked for by name, assumptions should not be made that the person answering the phone is the intended recipient;
7. Ensure you can confirm the identity of the caller before releasing any personal information;
8. Calls should not be made where they may be overheard by unauthorised individuals when passing on or receiving personal information;

9. Written telephone messages from individuals should be secured when left unattended and should not be available to anyone other than the intended message recipient;
10. When contacting service users/staff members by telephone consider the following:-
    i. Your service's standards on contacting service users/staff members by phone;
    ii. Whether the service user/staff member has consented to be contacted in this way;
    iii. The use of number withheld service to ensure anonymity;
    iv. Whether leaving personal information on answer phones is appropriate. Has the service user/staff member agreed to this?

4.10 Text

4.10.1 Due to increased use of mobile phones, transfer of information, especially individual information, is now being considered as a way of staff communicating with service users and other staff.

4.10.2 If a service is considering using text messaging as a way of communicating with service users/staff (i.e. appointment reminders), it is essential to seek guidance on any potential security, confidentiality and records management implications from the IG team and to have this agreed by the SIRO.

4.10.3 When transferring personal information by text, the following points should be adhered to:-

General

- Obtain the service users consent to be contacted in this way;
- Coded messages should be considered;
- All messages should be documented immediately and should then be treated as any other service user documentation

Texting from/to mobile phones

- A dedicated work phone must be used for the purpose of transferring this personal information;
- Named staff should be responsible for the dedicated phone(s) to maximise confidentiality;
- The mobile phone should be locked away when not in use;
- The mobile phone should have a passcode known only to the named staff members with responsibility for the phone;
- All received and sent messages should be deleted immediately from the dedicated phone after documentation;
- In the event of loss or theft of the mobile phone all precautions should be taken to protect the confidentiality of the service user and the theft/loss reported through the incident reporting process and to the police where appropriate.

4.10.4 Further guidance may be available from professional bodies in relation to the use of text messaging services e.g. RCN Use of text message services guidance for nurses working with children and young people.

4.11 **Fax – Appendix 4**

4.11.1 The recommended approach for the secure transfer of personal information by fax is to have a dedicated Safe Haven (see definitions). Although not every fax in the Trust will be designated Safe Haven fax, it is possible that the majority of these could potentially be used to send or receive personal information and as such should adhere to the principles below.

4.11.2 When sending personal information by fax ensure you adhere to the following:

- Use the MFD fax facility to transfer personal data;
- Ensure that you are using the correct fax number when sending a fax;
- If pre-programming numbers in your fax, ensure these numbers are tested by sending text faxes and receiving confirmation prior to their use;
- If not using pre-programmed numbers check and double check that you have typed the recipients number correctly;
- Use an appropriate cover sheet as agreed by your Directorate which should include the following:-
    - Marked “Confidential and Urgent”;
    - A standard security message;
    - Total number of pages that are being sent;
    - Contact details of the sender.
- Contact the intended recipient to ensure they are available and to allow them to prepare to receive the fax within an agreed timescale;
- Request that the recipient contacts you to confirm receipt or non delivery;
- Print a confirmation sheet for the transmission and file appropriately in line with professional record keeping;
- Once the fax has been printed, ensure that no records of this is left in the memory (check fax manual).

4.11.3 Misdirected faxes

4.11.3.1 If a fax is received in error contact the sender. The contents must not be disclosed to any other parties without the sender’s permission. Information received from a misdirected fax should be treated as highly confidential and should not be divulged to others. A misdirected fax can be received from internal and external sources.

4.12 Other Methods of transfer

4.12.1 This policy highlights the main ways in which personal information is likely to be transferred. However there may still be other methods in which information is transferred e.g. use of an outside contractor to support an office move which involves service user/staff information.

4.12.2 As with all the other methods described above, consideration must be given to any security and confidentiality risks of the method of transportation.

4.13 Transporting Personal Information (Appendix 5)

The following best practice guidelines are to be used when taking personnel information off-site:

i. Personal information should only be taken off-site when absolutely necessary or in accordance with local policy;
ii. Record what information is taken off site and why, and if applicable, where and to whom it is being taken;
iii. Packaging is to be sufficient to protect the contents from any physical damage likely to arise during transit such as exposure to heat or moisture i.e. an envelope for letters, jiffy bag for larger records, a secure box for larger packages etc;
iv. Information/packaging is to be kept out of sight;
v. Never leave personal information unattended eg: in a car overnight or during weekends;
vi. Ensure information is returned as soon as possible; and
vii. Record that the information has been returned.

4.14 Taking Personal Information Home

The following best practice guidelines are to be used when taking personal information home:

i. Ensure personal information is not seen by any other member of the household (including family, friends and neighbours) even if these people are employees of the Trust;
ii. It should be noted that the terms of conditions of employment, and the Trust's policies and procedures concerning security and confidentiality of information, apply to wherever the records are located. Information must only be accessed on a strict need to know basis; and
iii. Personal information (service user, staff etc) must not be recorded on any home PC as this compromises IT security and the security and confidentiality of the data. If an employee needs to work at home on a PC they should be provided with a laptop for this purpose and should seek advice from the ICT department concerning the responsibilities surrounding its use.

4.15 Personal Information Required by Medical/Dental Staff for Non-NHS Work

On occasion medical and dental staff may require access to service user records for private consultation work. The use of service user records in this way may compromise the individual's right to privacy under the Human Rights Act 1998 and the Data Protection Act 1998. In most cases this should only occur with the consent of the service user and the Trust's Data Guardian.

Medical/Dental staff wishing to have access to service user records for use in private consultation off Trust premises must adhere to the following:-

i. The records must be tracked on the Patient Administration system (PAS) indicating who the patient records have been taken by, for how long and where they can be located;
ii. Medical/Dental staff must be prepared to return patient records at short notice;
iii. Patient records must be transported in a way that confirms to the Trust's Policy for Safeguarding, Movement, Transportation of Patient/Client/Staff Trust Records and Other Media Between Facilities. Records must be put into the boot or secure area of the car. Medical/dental staff are fully aware that they have a legal responsibility to keep the records secure and confidential whilst in their care; and
iv. Medical/Dental staff must, in addition, comply with the requirements listed in paragraph 6.10 above.

4.16 Transporting Personal Information outside the United Kingdom

4.16.1 There are a number of other requirements and legal obligations surrounding the transfer of personal information outside the UK. If any service has a need to transfer information outside the UK they must first seek guidance from the Information Governance team.

4.17 Personnel Information Transferred to the Trust

The main focus of this policy is on transferring personal information held by the Trust, as this represents the biggest risk to Trust information. However staff also have a responsibility to protect personal information received into the Trust. The Trust would expect other organisations to implement similar levels of security around their information transfers. Where staff have concerns about the security of the information being received they should raise this with their line manager and if needed seek guidance from the Information Governance team.

5.0 IMPLEMENTATION OF THE POLICY

5.1 Dissemination

5.1.1 It will be the responsibility of the Information Governance Steering Committee to support the implementation of this policy across the Trust through action planning, awareness raising and training.

5.1.2 Line Mangers have a role to play in ensuring staff are aware of this policy and its implications.

5.1.3 All staff have a responsibility to adhere to this policy.

5.1.4 Staff will be trained in the transfer of personal information as per section 5.2.1

5.2 Resources

5.2.1 All staff will be required to have appropriate information governance training which will include guidance on transfer of personal information e.g. ICT induction, e-learning packages.

5.2.2 A range of training methods will be considered in relation to identified needs.

5.2.3 Other training and awareness raising around transfer of personal information will be arranged where appropriate.

5.2.4 This policy is available for all staff to access via the Trust's intranet. Staff without computer network access should contact their Line Manager for information on how to access this policy.

5.2.5 This policy will be included in the Trust's Publication Scheme in compliance with the Freedom of Information Act 2000.

5.3 Exceptions

5.3.1 This policy is applicable to all departments within the Trust.

6.0 USEFUL CONTACTS

The Information Governance Team
Lough House
Ards Hospital
Church Street
Newtownards, BT23 4AS
Tele No: 028 91512201

ICT Department
Trust Headquarters
The Ulster Hospital
BT16 1RH
Tee No: 028 9048 4511
Ext 3106/3107

7.0 MONITORING

This policy will be reviewed by the Information Governance Steering Committee on a 3 yearly basis or, as need arises due to national and regional guidance.

8.0 EVIDENCE BASE/REFERENCES

- Transferring Personal Information Policy & Procedures, Redbridge NHS Trust 07/02/08)
- Transfer of Personal Information Policy, Newcastle and North Tynesdie Primary Care Trusts and Northumberland Care Trust (13/03/08)
- ICT Security Policy, South Eastern HSC Trust (06/09)
- Policy for Safeguarding Movement, transportation of Patient/Client/Staff Trust Records and other media between Facilities (04/09)
- Data Protection Act 1998
- Human Rights Act 1998
- Use of Text Messaging Services: Guidance for Nurses working with children and Young People, Royal College of Nursing, 2006.
- DHSSPS Code of Conduct on Protecting Confidentiality of Service User Information (2009)

9.0 CONSULTATION PROCESS

The revision of this Policy has been consulted via the Information Governance Steering Committee.

10.0 APPENDICES/ATTACHMENTS

Appendix 1	Guidance for Emailing Personal Information
Appendix 2	Post for sending Personal Information by Post
Appendix 3	Guidance for Transferring Personal Information by phone
Appendix 4	Guidance for Transferring Personal Information by Fax
Appendix 5	Guidance for Transporting Personal Information

11.0 EQUALITY STATEMENT

In line with duties under the equality legislation (Section 75 of the Northern Ireland Act 1998), Targeting Social Need Initiative, Disability discrimination and the Human Rights Act 1998, an initial screening exercise to ascertain if this policy should be subject to a full impact assessment has been carried out.

In line with the Health & Social Care Board guidance on 'Making Communication Accessible for All' document this policy can be provided in alternative formats.

The outcome of the Equality screening for this policy is:

Major impact☐

Minor impact☐

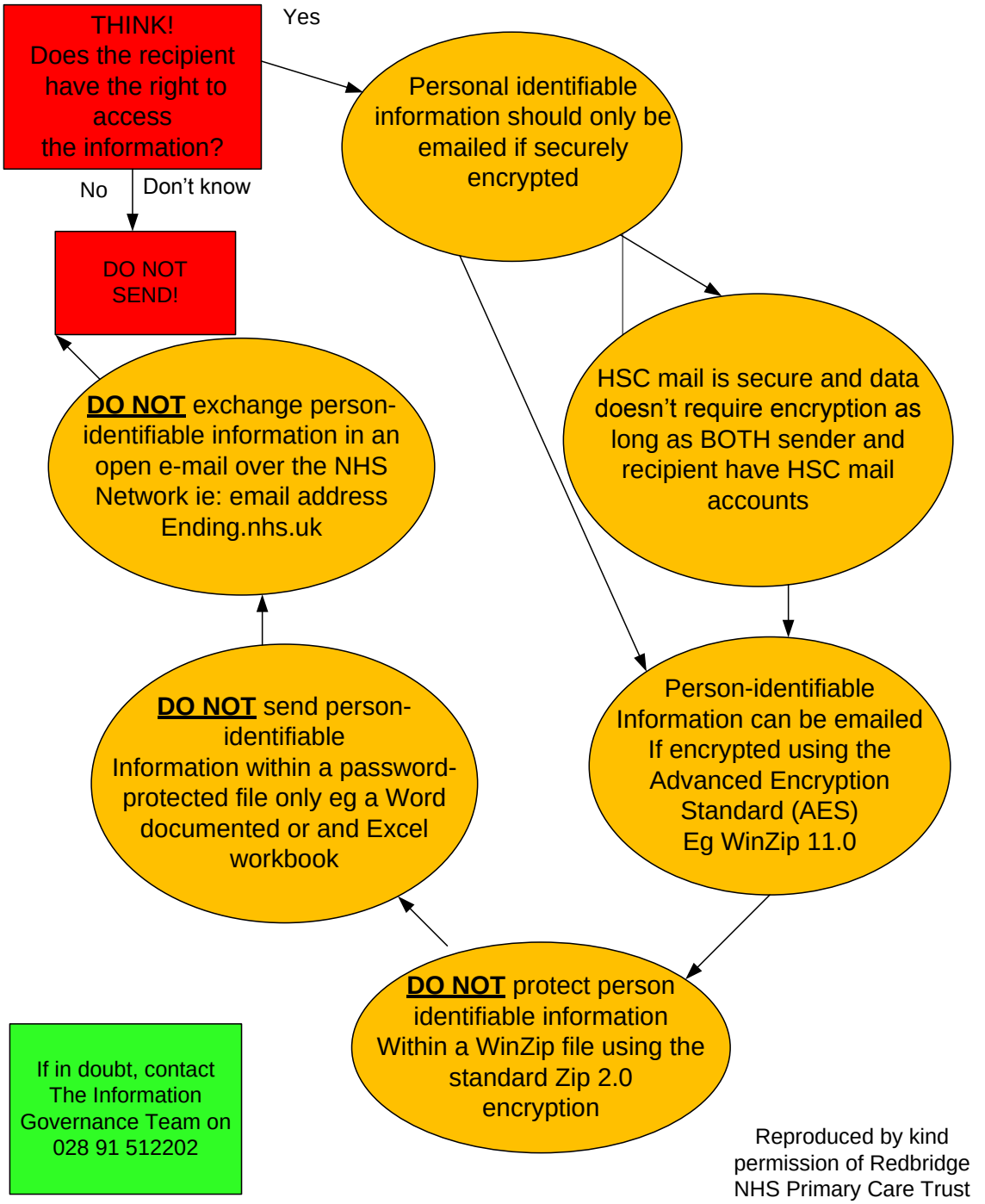
No impact. √

SIGNATORIES

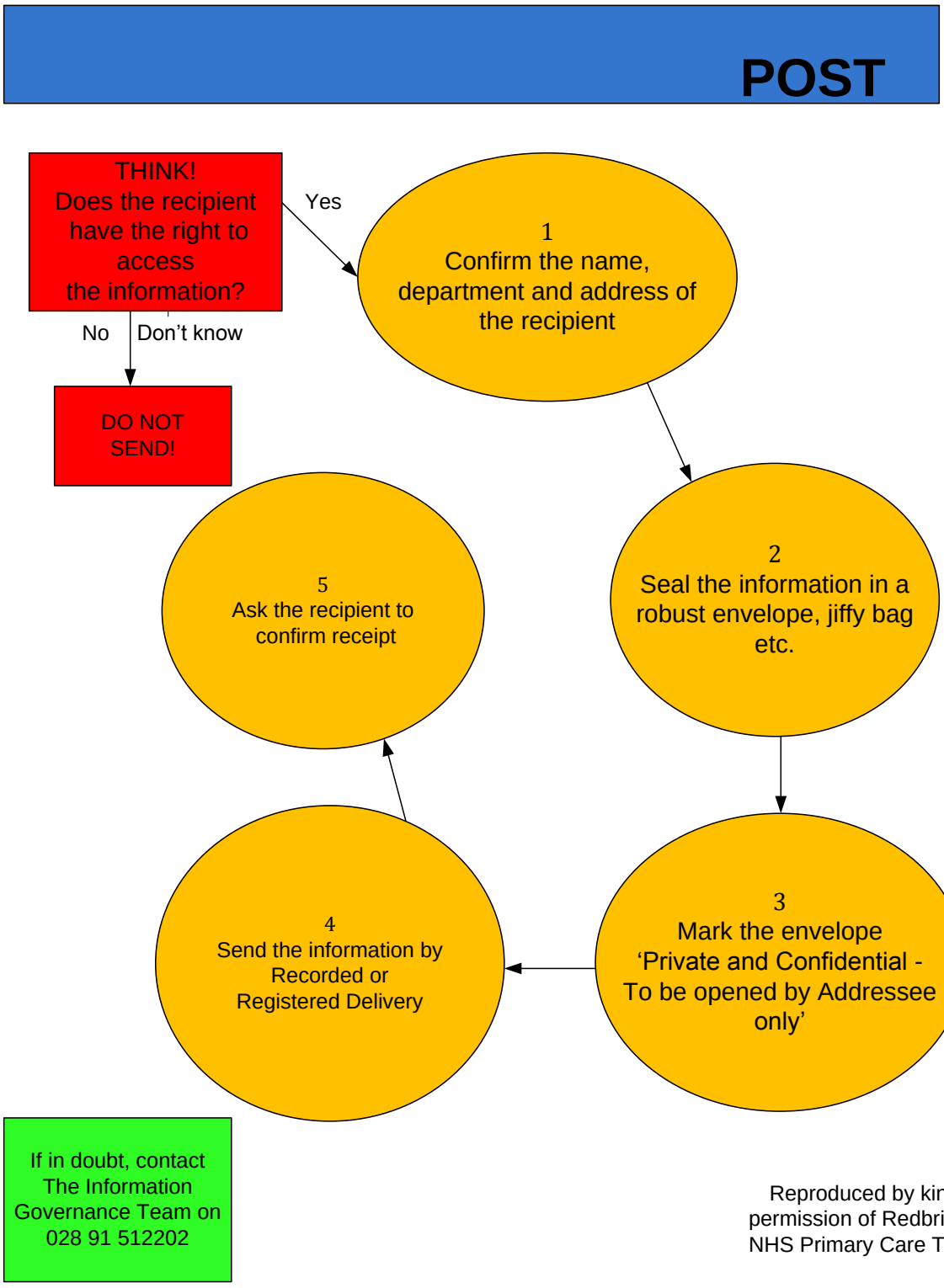
Form Status	Policy Name	Author Endorsement	Modified	Modified By
Directorate	Transferring of Personal Information	Yes	27/01/2015 05:06 PM	McAree, Lynda

Form Status	Policy Name	Approval	Modified	Modified By
Read Only	Transferring of Personal Information	Endorsed	15/05/2015 03:55 PM	Molloy, Eamonn
Read Only	Transferring of Personal Information	Endorsed	15/12/2015 03:28 PM	McCaughey, Hugh

Guidance for EMAILING personal information

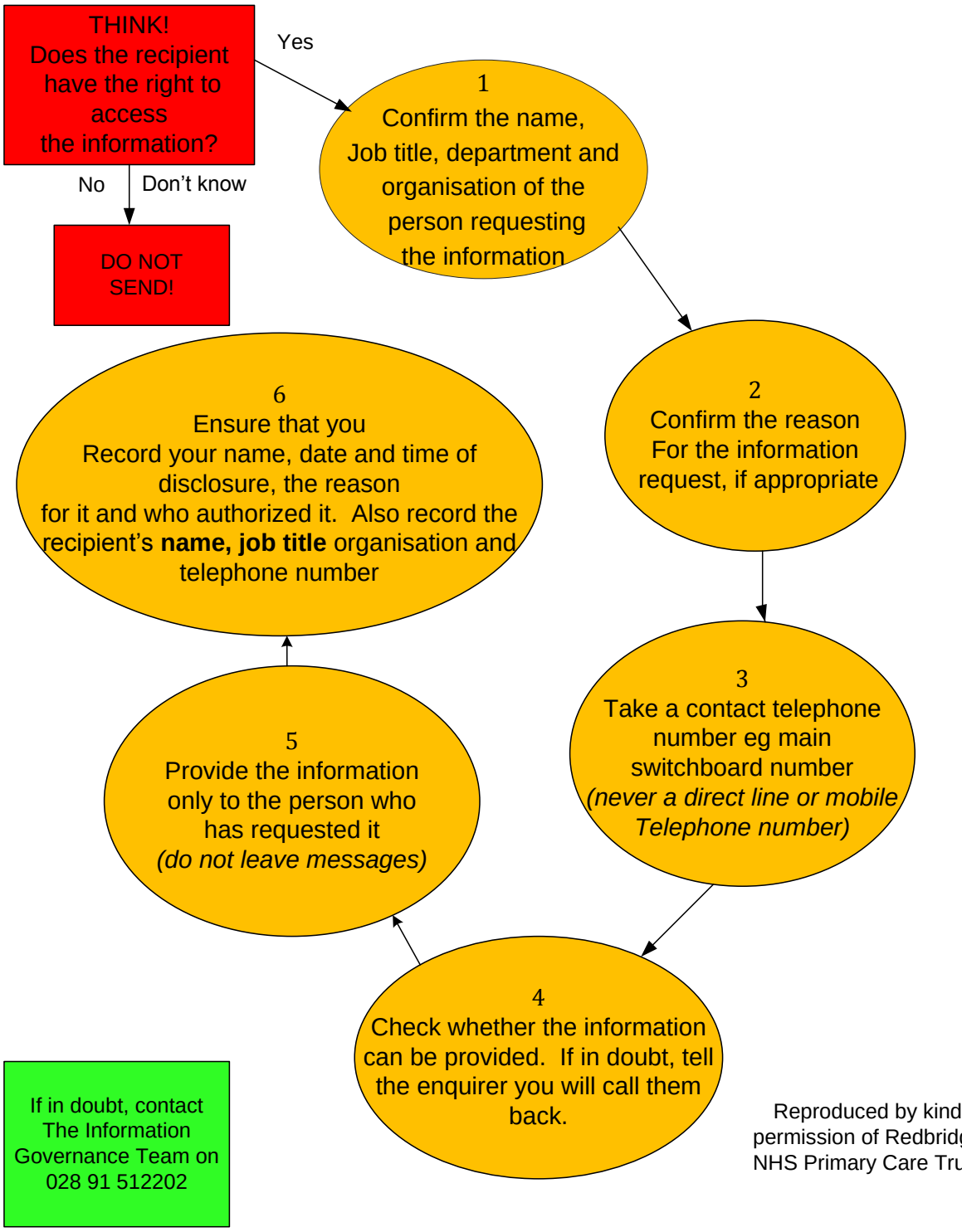


Reproduced by kind permission of Redbridge NHS Primary Care Trust



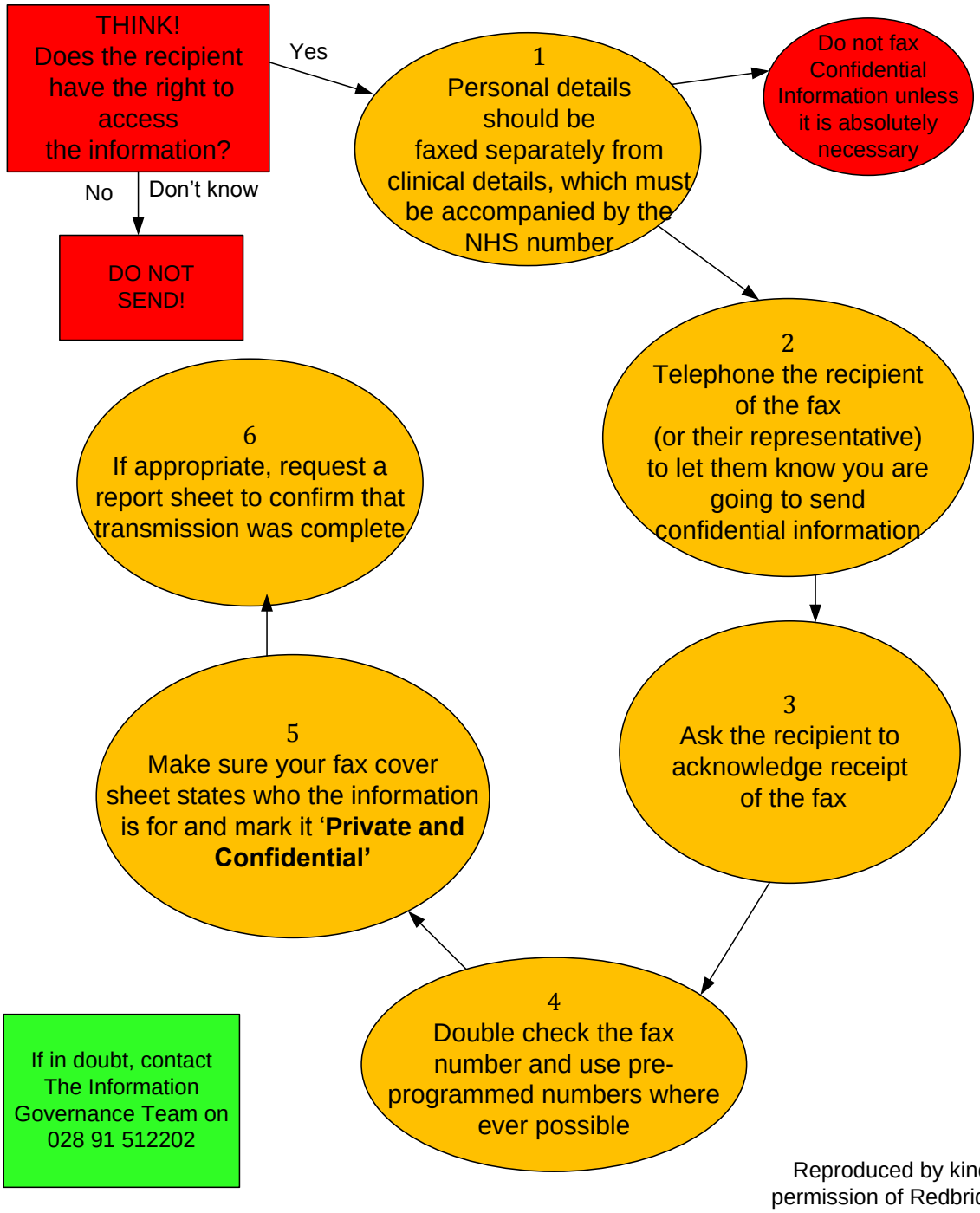
Reproduced by kind permission of Redbridge NHS Primary Care Trust

Guidance for transferring personal information by PHONE



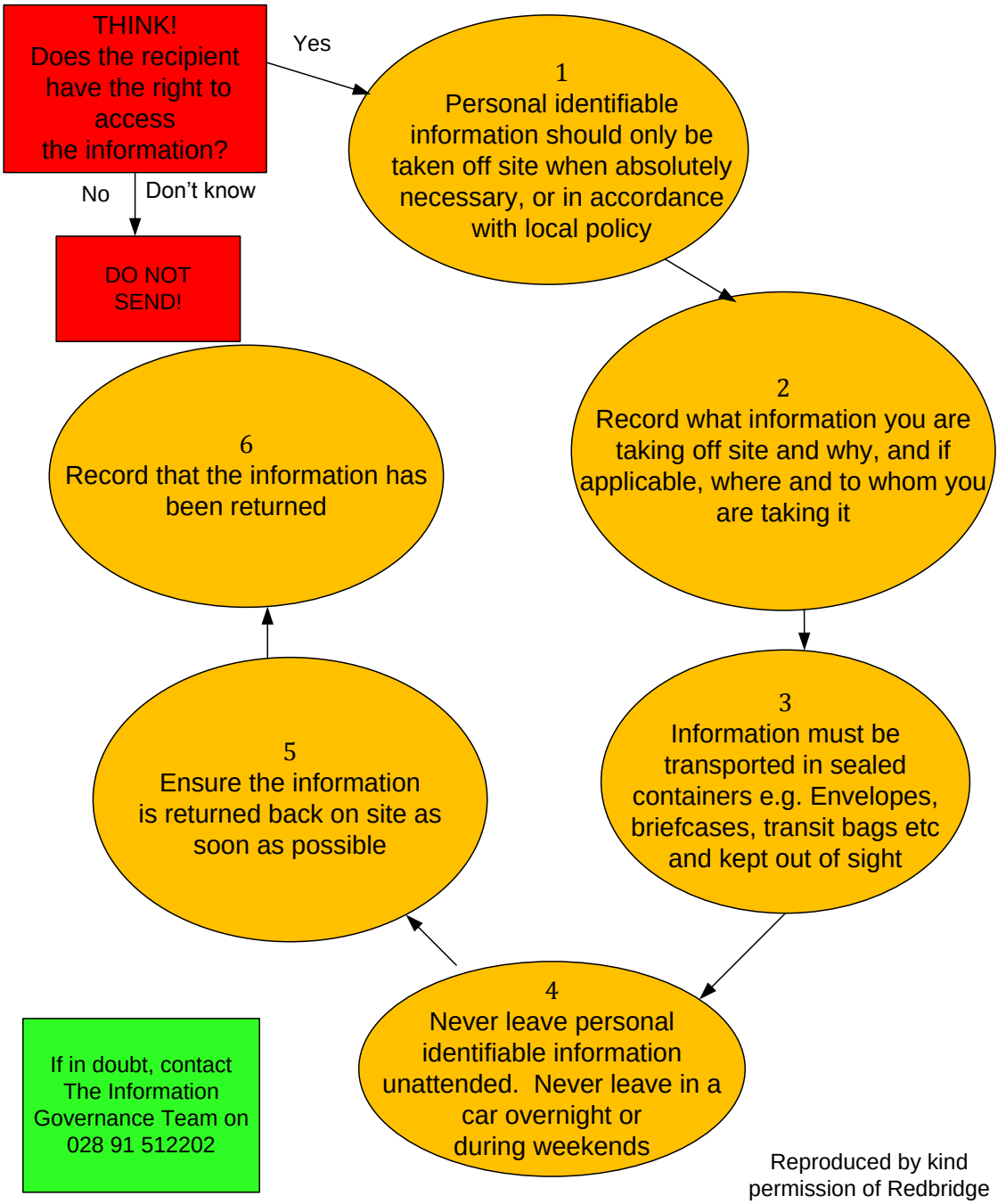
Reproduced by kind permission of Redbridge NHS Primary Care Trust

Guidance for transferring personal information by FAX



Reproduced by kind permission of Redbridge NHS Primary Care Trust

Guidance for TRANSPORTING personal information



Reproduced by kind permission of Redbridge NHS Primary Care Trust