Sheffield Health and Social Care
NHS Foundation Trust

Policy:

E-mail Policy

Exec Director lead	Clive Clarke
Author/ lead	SHSC Information Manager
Feedback on implementation to	SHSC Information Manager

Date of draft	16 February 2014
Consultation period	February – March 2014
Date of ratification	April 2014
Ratified by	EDG
Date for review	April 2017

Target audience	SHSC staff

Policy version and advice on availability and storage

Version 2.3
Available to all staff via SHSC intranet
Master copy held by Information Manager

Contents:

1. Introduction

E-mail is a widely used form of communication. It can be of great benefit to the Trust when used appropriately but its use also exposes the Trust to risks. These include non-compliance with various statutory requirements (for example, data protection legislation), threats to IT security and ineffective communication. The aim of this policy is to set out clearly the expectations of the Trust for the proper use of its e-mail system, and e-mail accessed via Trust systems, as required by the Trust's Information Governance Policy.

2. Definitions

For the purposes of this policy, e-mail includes the e-mail system provided by the Trust, however it is accessed, and NHSmail (formerly known as NHSContact).

3. Purpose of this Policy

The purpose of the policy is to ensure the appropriate and effective use of e-mail on Trust systems by:

- Setting out the rules governing the sending, receiving and storing of e-mail.
- Establishing Trust and user rights and responsibilities for the use of the system.
- Promoting adherence to current legal requirements and NHS information governance standards.

4. Duties

Users will be required to read the policy and sign a declaration that they have understood it and agree to abide by its content prior to receiving access to the e-mail system.

Failure to comply with this policy and procedures may have serious consequences for the individual including civil, criminal and/or disciplinary proceedings.

5. Scope of this Policy

This policy applies to the following areas:

- All users of the Trust system including Trust employees and non-Trust employees who have been authorised to use the system.
- Use of the Trust e-mail system for business and personal use on Trust and non-Trust premises including from home and internet cafes and via mobile devices.
- The use of NHSmail accounts.

6. Policy

6.1 Trust responsibilities and rights

6.1.1 Access to and use of e-mail systems

The Trust provides access to electronic systems to employees and authorised non-Trust employees only for use in their:

- Work duties
- Work related educational purposes
- Work related research purposes

The Trust allows short communications of a personal nature although the personal use of e-mail as a general practice is discouraged due to the detrimental effect it may have on Trust business.

No-one has a right of access to an e-mail account. The inappropriate use or abuse of e-mail may result in access being withdrawn or amended.

The Trust reserves the right to remove or amend access to the e-mail system at any time in order to protect and preserve the integrity and confidentiality of the system.

The Trust will:

- Provide users with appropriate training in the use of e-mail.
- Provide the appropriate and authorised software for e-mail.

6.1.2 Monitoring

- Any information held or passing through the e-mail system is the property of the Trust.
- All e-mail sent or received via NHS systems is monitored for viruses.
- All e-mail (incoming and outgoing) is logged automatically.
- Monitoring logs are audited periodically.
- The use of e-mail is not private. The content of e-mail is not routinely monitored but the Trust reserves the right to access, read, print or delete e-mails at any time.
- Any monitoring or interception of communications will be carried out in accordance with legislation such as the Regulation of Investigatory Powers Act 2000, the Data Protection Act 1998, the Human Rights Act 1998 and the Trust policy regarding monitoring and privacy.

6.1.3 Retention and destruction policy

- The Trust reserves the right to retain e-mail as required to meet legal and statutory obligations.
- E-mail stored on Trust servers will automatically be deleted in accordance with the Trust's records management policy.
- Where the content of e-mail may be needed in the future it is the responsibility of the user to ensure it is stored appropriately, separately from the e-mail system.
- E-mails and attachments that do not relate to work activities or do not need to be kept as part of a record must be deleted as soon as possible after receipt.
- E-mail is a communication tool and not a record management system. Where the content of e-mail or attachments forms part of a record it is the responsibility of the user to ensure it is added to, and becomes part of, that record whether held in hard copy or electronic format.

6.1.4 Breaches of this policy

The Trust will:

- Investigate breaches of this policy, actual or suspected, in accordance with Trust procedures.
- Where appropriate, invoke the Trust's disciplinary procedure for breaches of this policy.
- Where appropriate, make a complaint to an individual's employing organisation and co-operate fully with any investigation of that complaint where breaches of this policy are committed by users who are not employees of the Trust (such as staff on secondment to the Trust, Honorary Contract holders and users given access to systems by agreement between the Trust and the user's employing organisation).
- Where appropriate, take legal action (that is, criminal or civil proceedings) in respect of this policy.
- Where appropriate, suspend the users account until the investigation has been completed. The user may be required to complete the nationally provided online e-learning information governance training before the account is re-enabled.

6.1.5 Liability

The Trust will not be liable for any financial or material loss to an individual when using e-mail for personal use.

6.2 User responsibilities and rights

6.2.1 Access to and use of e-mail systems

Users should write e-mail messages on the assumption that they may be read by others. A concise, meaningful title must be put in the subject heading of every e-mail to indicate its content. (This will assist the recipient in prioritising the opening of e-mail and aids the retrieval of opened messages).

Where important information has been sent by e-mail, confirmation of receipt should be obtained either by e-mail or by a follow up telephone call.

Users must respond to e-mail messages in a timely manner.

Users must ensure that their e-mail inboxes do not become full – any messages sent to a full mailbox will be lost.

Users must not use automatic rules to delete e-mails unread.

Where users wish to attach a standard disclaimer in the footer of an e-mail they must only use a disclaimer that has been authorised by the Trust (contact the SHSC Communications Department for advice).

Inappropriate use of e-mail may result in poor communication, impede the function of the Trust's network system, impede the effective functioning of e-mail, or compromise the security of the system.

6.2.2 Legal requirements

The use of e-mail must comply with the law such as the Data Protection Act 1998 and adhere to Trust rules, codes of conduct, policies and procedures such as this policy, and those covering equal opportunities and anti-harassment.

Users must comply with any licence conditions and copyright for any software they have access to.

Users must not use e-mail for any purpose that conflicts with their contract of employment.

Users must not agree to terms or enter into contractual commitments or make representations by e-mail without having obtained the proper authority (a typed name at the end of an e-mail is just as much a signature as if it had been signed personally).

The content of any e-mails may be disclosable under the Freedom of Information Act 2000. As such e-mail messages must not include anything that would offend or embarrass any reader or would embarrass the Trust if it found its way into the public domain.

E-mail messages have the same legal status as other written documents and must be disclosed in legal proceedings if relevant to the issues.

Improper statements may result in the Trust and/or user being liable under law.

6.2.3 Security

All passwords and log in details for e-mail systems must be kept confidential. Sharing passwords or login details will be considered misconduct. Where necessary, users can give proxy access to their e-mail account.

Users must log off the Trust network or lock their terminal when not at their computer for a protracted length of time – for example to attend a meeting or to go for lunch.

Portable devices, including mobile and smart phones, used to store e-mails, must be encrypted.

6.2.4 Confidential information

Confidential or sensitive information, including information about service users and staff, must not be sent outside the Trust by unencrypted e-mail.

Do not send confidential information via e-mail unless it is absolutely necessary. Use anonymised information whenever possible and where it is necessary to include person-identifiable information use the minimum necessary.

Where it is necessary to send person-identifiable information from a SHSC e-mail address (ending in @shsc.nhs.uk) the text "[encrypt]" **must** be included in the subject line. The square brackets are part of the mandatory text. Any such messages will then be encrypted if they pass outside the boundaries of the SHSC network. The recipient will then be required to register with a secure website to generate a password which will allow the encrypted message and any future encrypted messages from the Trust to be opened. Messages sent by replying to an encrypted e-mail will also be encrypted. A password will not be required to open messages sent within the Trust or the City Council network but the "[encrypt]" text must still be included to protect the message should it be forwarded outside the network. A guide on using this encryption facility is available on the Intranet.

Sheffield City Council has its own policy on how confidential information may be sent via e-mail – check with the intended recipient before sending.

Messages sent from NHSmail e-mail addresses (ending in @nhs.net) are encrypted during transmission to other NHSmail addresses and to certain other public sector addresses belonging to linked networks (see Appendix B for the list of linked networks). Some public sector organisations insist on the use of NHSmail addresses for the transfer of person-identifiable information – the IT Department can advise on how to get a NHSmail account.

To provide added protection when sending information within the Trust it can be attached to the e-mail as a password-protected document. When using this method make sure that the password is given to the recipient separately, not included in the same message.

Confidential or sensitive Trust information must not be processed on non-NHS devices without authorisation from the IT Department. Where members of staff process information under Bring Your Own Device (BYOD) arrangements the device must be protected in line with Trust requirements which include the facility to wipe information remotely if the device is lost.

Any computer that is used for work purposes must be protected by up to date, approved anti-virus software. (Advice about anti-virus software can be obtained from the IT Help Desk).

6.2.5 Referrals by E-mail

E-mails sent from NHSmail addresses to SHSC addresses are not encrypted in transit but they are conveyed via the NHS N3 network which is considered secure so GPs may send referrals via e-mail to the publicised generic team e-mail addresses if their own policies allow.

6.2.6 E-mail correspondence with Service Users or Carers

Some service users or carers may request SHSC services to correspond with them via e-mail. This will be quicker and cheaper than traditional post but it also introduces some risks that the service user must be made aware of.

E-mail communication is not a substitute for face to face or telephone contact with service users because there is a lack of interaction – we will not always know whether an e-mail has been read and if it has, we cannot be sure who has read it.

SHSC has no control over access to the service user's PC. E-mails will be encrypted as long as the text "[encrypt]" is included in the subject line as described above but the recipient is responsible for who has access to their PC and what they do with the password generated by the encryption software. They are also responsible for the secure storage and eventual disposal of any e-mails they receive, whether in electronic or printed format.

If service users request communication via unencrypted e-mail they must be made aware of and accept the higher risk of unauthorised access to messages. By default e-mails sent to service users should be encrypted.

SHSC cannot verify that e-mails sent from the service user's e-mail address are genuine in the event that another person has access to their account so it is the service user's responsibility to protect their account from unauthorised use.

The service user is responsible for checking their e-mail regularly to make sure they read messages promptly and to make sure that messages are not lost because their in-box is full.

The service user must inform the Trust if they change their e-mail address or if they no longer wish to receive e-mails from the Trust.

If a service user requests that SHSC services correspond with them via e-mail the risks of doing so must be explained to them and the service user will be required to sign a form to confirm that they understand and accept the risks – see Appendix C

If it is decided that e-mail communication is detrimental to the treatment of a service user or to the operation of a service then the Trust may refuse to communicate with the service user by e-mail. Any such decision and the extent of the restriction must be approved by an executive director in consultation with the Trust Complaints and Litigation Lead.

Service users should only send e-mails to the agreed generic team address to ensure that their messages are read in the event of a member of staff being absent. The service user will be given the generic e-mail address on submission of the form described above. Teams which agree to communicate with service users via e-mail will ensure that the designated e-mail addresses are checked regularly and messages dealt with but service users will be prioritised according to clinical need so sending a message via e-mail does not guarantee an immediate response.

Any information transmitted by e-mail which is part of the care record must be copied and pasted into a note on the Care Record module of Insight or stored in the appropriate system where services do not use Insight. The e-mail system should not be used as a document management system.

6.2.7 Personal use

The personal use of e-mail is permitted as long as messages are sent in the user's own time, they do not detract from the user's work duties and they do not disrupt the work of others.

Personal e-mails should be stored in a folder marked ‘personal’ and should be marked as ‘personal’ in the subject header.

6.2.8 Forwarding mail

Users must not automatically forward mail from their Trust e-mail account or send confidential or sensitive Trust information to their own non-NHS e-mail accounts. Examples of non-NHS e-mail accounts include Hotmail, G-mail and e-mail services provided by internet service providers.

6.2.9 Misuse of the system

Users must not:

- Use the Trust’s e-mail to conduct private or freelance work for the purpose of commercial gain.
- Create, hold, send or forward e-mails that have obscene, pornographic, sexually or racially offensive, defamatory, harassing or otherwise illegal content (if you receive such a message you should report it to the IT Help Desk immediately).
- Create, hold, send or forward e-mails that contain statements that are untrue, inaccurate, misleading or offensive about any person or organisation.
- Access and use another user’s e-mail account without permission. (If it is necessary to access another user’s account then contact the IT Help Desk for details of the necessary procedure. Users should be aware that access to their email account by authorised individuals may be necessary in periods of absence for business continuity reasons).
- Send e-mail messages from another member of staff’s e-mail account or under a name other than their own. (Secretaries/PAs may send e-mails in their own name on behalf of their manager if instructed to do so).
- Use e-mail for political lobbying.
- Knowingly introduce to the system, or send an e-mail or attachment, containing malicious software, for example, viruses.
- Forge or attempt to forge e-mail messages, for example, “spoofing”.
- Send or forward chain letters or other similar non-work related correspondence.
- Send unsolicited e-mails (spam) to large numbers of users unless it is directly relevant to the recipient’s work. (Use staff bulletin/notice boards where appropriate).

6.2.10 Attachments

Users must not send or forward large messages or attachments. 10Mb is an absolute limit but good practice is below 1-2Mb. (Examples of large attachments include photographs, large documents, electronic greetings and flyers).

The sending and storing of large attachments can cause the Trust network to slow down or crash and can seriously affect the Trust’s capacity to store files.

If it is necessary to send large attachments, consider if it is possible to break them down into several smaller files to be sent separately. If photographs must be sent as attachments, sending them in jpeg (.jpg) format makes them much smaller than bitmap (.bmp) format.

Consider alternative ways of making large work documents available to colleagues such as placing documents on the intranet or server and e-mailing a link. Alternatively, use file compression, for example, ‘zip’ files, or other methods of file transfer, for example, FTP. (Ask the IT Help Desk for advice).

7. Dissemination, storage and archiving

This policy will be made available to all staff via the SHSC intranet. All new e-mail users will be made aware of the policy when they receive training and issuing of an e-mail address will be conditional on their acceptance of the policy.

Changes to this policy will be made by the SHSC Information Manager at the request of or approved by the Information Governance Steering Group (IGSG).

8. Training and other resource implications

Departmental managers are responsible for ensuring that their staff are aware of and comply with this policy when using e-mail. This policy will be referenced during e-mail training, as were previous versions of the policy.

9. Audit, monitoring and review

Compliance with this policy will be judged by the appropriate working group as part of the annual Information Governance Toolkit assessment for the Trust.

Instances of non-compliance will be identified by the Trust's incident reporting procedures.

The policy will be reviewed periodically. Review of the policy is the responsibility of the Information Governance Steering Group.

10. Implementation plan

On approval by the Executive Directors Group, the revised policy will be made available via the policies section of the SHSC intranet. New starters will be informed of relevant policies by their departmental managers.

11. Links to other policies

This policy forms part of an overall suite of information governance policies and should be read in conjunction with the Information Security Policy in particular.

12. Contact details

Questions on the operation of this policy should be directed to the Director of IM&T in the first instance. Requests for changes to the policy should be directed to the Information Manager. Both are based at Fulwood House.

13. References

This policy is a requirement of the Information Governance Toolkit

Details of the toolkit can be found at https://nww.igt.hscic.gov.uk/

14. Policy development and consultation process

This policy was originally developed by the city-wide Information Governance Group (SCT and PCTs).

It was tabled at the SCT Information Governance Committee.

It was sent, along with other IG policies to JCF in June 2007 (in light of the heavy workload due to the Foundation Trust application, the policies were considered outside the meeting by staff side).

Following consultation with staff side, the policies were agreed by the Information Governance Committee in September 2007.

The e-mail attachment size limit was increased and advice on sending large attachments was added as a result of consultation within the SCT IT department and in light of enhanced network capabilities in March 2008.

The policies were re-formatted in line with revised Trust requirements.

This policy was augmented in light of national guidance on information security, data flows and encryption in March 2008.

The policies in new format were approved by the Information Governance Committee on 10 March 2008.

The policies were approved by the Performance Information Group on 18 March 2008.

The policy was reviewed and amendments made (including the replacement of Appendix B) in October 2010.

Further amendments made following submission to the Information Governance Steering Group, then submitted to the Performance Information Group.

Reviewed and amended by the IGSG, section on e-mailing confidential information revised and section on e-mailing to service users added, 20 November 2012.

Reference to BYOD devices added, Appendix C wording clarified and paragraph on default encryption to service users added, 30 November 2012.

Reviewed and minor amendments made by the IGSG, February 2014

Appendix A Guidance on the Use of E-mail

Do:

- Check e-mail regularly, for instance twice daily if possible, and respond to requests promptly.

- Advise people when you will not able to read your e-mail (e.g. when on annual leave) by using an Out of Office message.

- Be careful when giving out your e-mail address. Avoid subscribing to mailing lists where possible, and only subscribe to legitimate work related mailing lists (although even these can be used by spammers).

- Avoid posting your e-mail address unnecessarily on web pages – these can be harvested by spammers.

- Be selective about who receives your e-mails especially when using:
  "Reply to all" - consider whether all recipients need to see the reply
  Distribution lists – is it important that everyone on the list receives your e-mail?

- If you have to send an e-mail to a distribution list involving large numbers of staff, send it as a blind copy, that is, put the distribution list in the 'Bcc' field. If the e-mail is not blind copied, individual e-mail addresses will be visible to all recipients which may compromise a recipient's confidentiality – this will be a particular issue if service users are included as well as staff. Large lists of e-mail addresses can also detract from the actual message and are wasteful if printed out.

- Consider putting a document on the intranet and e-mailing a link to it rather than sending the document itself. Alternatively, consider putting the document in a shared folder on a server.

- Consider if information contained in an attachment could be sent in the text of an e-mail rather than sending it as an attachment – this makes the message smaller.

- Use e-mail only when it is appropriate and not as a substitute for verbal communication.

- Exercise as much caution in what is said in e-mail messages as would be exercised in more formal correspondence.

- Write all e-mails as if a third party will read them. E-mail is easily forwarded and may be read by unintended recipients.

- Word e-mails with care because voice inflections cannot be picked up and it can be difficult to interpret the tone.

- Check each e-mail before despatch. Once you have clicked the send button e-mails often cannot be retrieved.

- Use the "high priority" setting only for messages that are genuinely urgent and require a fast delivery.

- Save important e-mails as text documents in Word or as part of an appropriate record.

- Delete messages that you no longer need and archive messages regularly.

- Check the non-delivery report, where an e-mail is returned as undelivered, for the reason for non-delivery before asking IT Help Desk for help. It may be that something simple like correcting the address is all that is required.

Do Not:

- Be caught out by the speed of e-mail. E-mail is quick and easy to use and can result in ill-considered, brief and even offensive messages. Before replying to a message consider if your first reaction is the one you want the recipient to receive.

- Use e-mail as the only method of communication if an urgent response is required.

- Send or forward private e-mails at work, which you would not want a third party to read.

- Type messages in capital letters. Using capitals may be perceived as aggressive.

Malicious software

Beware of malicious software, that is, computer viruses, worms and trojans. These are small computer programmes intended to damage, destroy or steal information from your computer. They can be devastating and very expensive to deal with. Information can be permanently lost. E-mail, the internet and the interchange of removable media are common ways of distributing malicious software.

You can reduce the risk of malicious software by:

- Not opening e-mail attachments unless you are certain that they are from a trusted source.

- Not opening e-mail that does not have a subject heading or if the subject heading is unusual or inconsistent with what you would normally expect from the sender.

- Saving e-mail attachments to disc and scanning for viruses before opening, particularly if received from an external source.

- Reporting any suspicions to the IT Help Desk.

Remember

The content of any e-mails may be disclosable under the Freedom of Information Act 2000 or in answer to a subject access request.

E-mail messages have the same legal status as other written documents and must be disclosed in legal proceedings if relevant to the issues.

Improper statements may result in the Trust and/or user being liable under law.

Who should I contact if I have a problem?

Any questions about the appropriate use of e-mail should be directed to your line manager in the first instance. If, after doing so, you still have questions then you should contact the Trust's Information Governance Lead.

Questions about the use of the system or any problems in accessing e-mail should be directed to the IT Help Desk

Appendix B Guidelines on sending confidential information via e-mail

The preferred method of sending confidential information within the NHS is via NHSMail. This is a national system provided for the NHS where any messages are encrypted in transmission as long as both the sender and the recipient use NHSMail addresses.

NHSMail is not the same as the ordinary Microsoft Outlook e-mail system used by SHSC. NHS mail addresses end in ".nhs.net" instead of ".shsc.nhs.uk". E-mail which is sent to or from a SHSC e-mail address is not encrypted by default and so should only be used to transfer non-confidential information unless it is additionally protected by including the text "[Encrypt]" in the subject line.

Any member of NHS staff can apply for a NHSMail account via the website:

https://web.nhs.net

SHSC staff experiencing difficulty in obtaining a NHSMail address should contact the IT Help Desk.

The NHSMail system also has links to other secure public sector e-mail systems which allow confidential information to be sent to e-mail addresses in any of the following domains:

GCSX (*.gcsx.gov.uk)	GSI (*.gsi.gov.uk)
SCN (*scn.gov.uk)	CJX (*.police.uk or .pnn.police.uk)
CJSM (*cjsm.net)	GSE (*.gse.gov.uk)
MoD (*.mod.uk)	GSX (*.gsx.gov.uk)

SHSC staff who register for a NHSMail address should be aware that they may receive e-mails to either address and should make it clear which address they wish to be used. They should check both inboxes regularly since mail could be sent to either.

Where it is necessary to send confidential information but sender and recipient do not both have and cannot obtain secure addresses (NHSMail or one of the systems listed above) then e-mails sent from a SHSC address may be encrypted by including the text "[Encrypt]" in the subject line. E-mails sent by replying to such a message will also be encrypted – a help sheet is available on the SHSC intranet.

Any other transfer of confidential information via e-mail which does not conform to these requirements must be approved by the Information Governance Steering Group before it may commence.

Appendix C Agreement to Receive E-mail Correspondence

Ordinary e-mail accounts are not secure. Although NHS e-mail systems are protected by security measures Sheffield Health and Social Care has no control over what happens to a message once it leaves our systems. Copies of e-mails may be retained on servers during transit and we have no control over who you forward e-mails to, nor who you allow to look at e-mails on your computer or in printed form.

If you wish us to communicate with you via e-mail we will not include confidential information unnecessarily but details of your condition (or that of the person you care for) or the services you use may have to be included or may be apparent from details in the e-mail or the sender's details.

Sheffield Health and Social Care cannot accept responsibility for the security of any information sent by e-mail once it has left our systems. You are responsible for controlling who can access your e-mail account and any information stored on your computer or forwarded or printed by you.

Sheffield Health and Social Care has implemented software which encrypts e-mails sent outside the Trust network. The first time you receive one of these e-mails you will need to log on to a secure server in order to generate a password which will allow you to open the encrypted e-mails. Any replies to an e-mail encrypted in this way will also be encrypted.

You can ask us to stop sending you e-mails at any time.

You must tell us if the e-mail address that you want us to use changes at any time.

If we suspect that e-mail communications have been inappropriately accessed or misused in any way we reserve the right to stop using e-mail to communicate with you. We also reserve the right to discontinue e-mail correspondence if in our judgment the system is abused or it becomes detrimental to your care.

In order to make sure that any e-mails you send are dealt with in a timely manner it is important that any e-mails you send are to the agreed team e-mail address rather than to a particular member of staff.

If you wish us to communicate with you via e-mail subject to these conditions, complete the form below and give the original document to your worker.

Name: _____

Address: _____

_____

_____

Position: Service user / Carer / other Representative
(delete where not applicable)

If you are not the service user, give their details here:

Name: _____

Address: _____

_____

_____

I understand and accept the risks involved in the use of e-mail and I wish Sheffield Health and Social Care NHS Foundation Trust to communicate with me in this way until further notice.

Signed: _____

Date: _____

.

E-mail address to be used for correspondence with the person requesting this communication:

_____

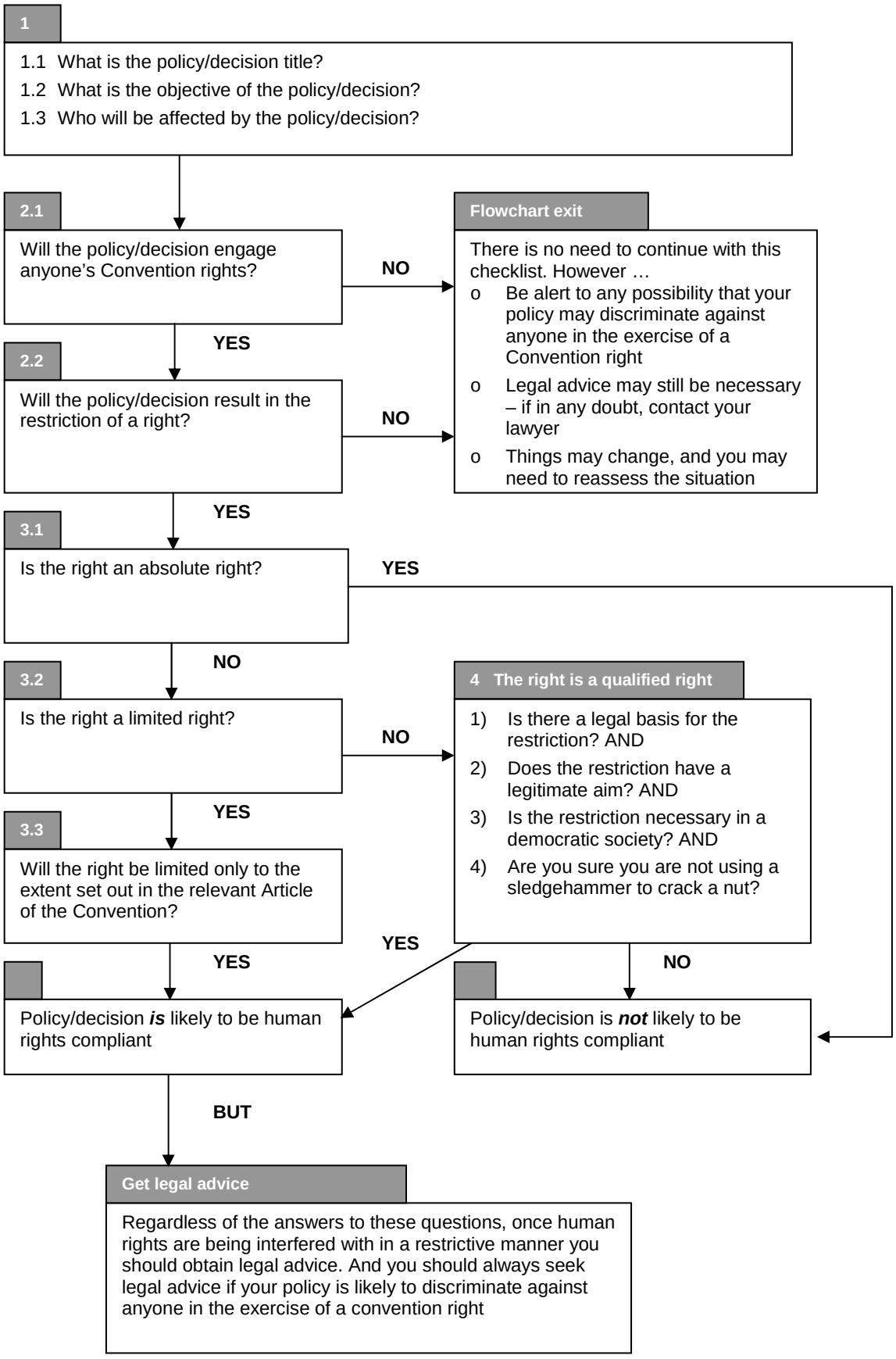
Appendix D Equality Impact Assessment Form

To be completed and attached to any procedural document when submitted to the appropriate committee for consideration and approval.

		Yes/No	Comments
1.	**Does the policy/guidance affect one group less or more favourably than another on the basis of:**		
	• Race	No	
	• Ethnic origins (including gypsies and travellers)	No	
	• Nationality	No	
	• Gender	No	
	• Culture	No	
	• Religion or belief	No	
	• Sexual orientation including lesbian, gay and bisexual people	No	
	• Age	No	
	• Disability - learning disabilities, physical disability, sensory impairment and mental health problems	No	
2.	**Is there any evidence that some groups are affected differently?**	No	
3.	**If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?**	N/A	
4.	**Is the impact of the policy/guidance likely to be negative?**	No	
5.	**If so can the impact be avoided?**	N/A	
6.	**What alternatives are there to achieving the policy/guidance without the impact?**	N/A	
7.	**Can we reduce the impact by taking different action?**	N/A	

If you have identified a potential discriminatory impact of this procedural document, please refer it to Liz Johnson (Head of Patient Experience Inclusion) together with any suggestions as to the action required to avoid/reduce this impact.
For advice in respect of answering the above questions, please contact Liz Johnson (Head of Patient Experience Inclusion and Diversity)

Appendix E Human Rights Act assessment checklist



What is the policy/decision title?
E-mail Policy

What is the objective of the policy/decision?
To ensure the appropriate and effective use of e-mail on Trust systems

Who will be affected by the policy/decision?
Users of Trust e-mail systems (including users of NHSmail within the Trust)

Will the policy/decision engage anyone's Convention rights?
Yes. Article 8 Right to Respect for Private and Family Life covers employees' rights to privacy including the monitoring of e-mails and telephone calls

Is the right an absolute right?
No

Is the right a limited right?
Yes

Will the right be limited only to the extent set out in the relevant Article of the Convention?
Yes. Use of e-mail is only restricted or monitored for the prevention of crime, the protection of health or morals or the protection of the rights or freedoms of others.

Policy/decision is likely to be human rights compliant