NHS
Yorkshire
Ambulance Service
NHS Trust

Email Policy

Document Author: Infrastructure, Development and Systems Manager

Date Approved: September 2016

Document Reference	PO – Email Policy
Version	4.2
Responsible Committee	Trust Management Group
Responsible Director	Executive Director of Finance
Document Owner (title)	Associate Director of ICT
Document Lead (title)	Infrastructure, Development and Systems Manager
Approved by	Trust Management Group
Date Approved	September 2016
Review date	June 2019
Equality impact assessed (yes/no) (full/screening)	No
Protective Marking	Not protectively marked

Document Control Information

Version	Date	Author	Status (A/D)	Description of Change
1.0	March 2008	David Johnson	A	Initial policy developed.
2.0	March 2011	David Johnson	A	Revisions to format and content.
2.1	Oct 2012	Ola Zahran	D	Existing email procedure checked for any amendments, formatting changes
2.2	Feb 2013	Caroline Squires	D	Significant revisions to existing procedural document in relation to content and format. Redefined existing procedures as policy with best practice incorporated.
2.3	April 2013	Caroline Squires	D	Amendments in response to consultation with Information Governance Working Group members.
3.0	May 2013	David Johnson	A	Following SMG May 2013
3.1	May 2016	Ola Zahran	D	Update reference to Email acceptable use policy in body of policy. Change SMG to TMG.
3.2	Aug 16	Maxine Travis	D	Insert Staff Summary table
4.0	Sep 16		A	TMG
4.1	Feb 18	Risk Team	A	Documents formatted – New visual identity
4.2	Feb 19	Ola Zahran	A	TMG approved extension of 3 months. Review date amended to June 2019
A = Approved D = Draft				
Document Lead = Infrastructure, Development and Systems Manager				
This document is controlled. If you would like to suggest amendments to this document please contact the document author				

Staff Summary

The Email Policy outlines the permissible, acceptable, use of business email when accessing YAS email services from the workplace or when using network services remotely
The Policy sets out prohibited use of email
It provides best practice guidelines to make the most effective and secure use of the email system for both internal and external email communications
The policy applies to all employees of Yorkshire Ambulance Service NHS Trust including contractors, bank, agency and temporary staff as well as volunteers who use YAS email
Policy covers all email (eg. outlook) and other similar communication systems used by the Trust, including Clinical Hub, GRS, Cleric PTS and Adastra systems which all provide some messaging functionality
All data retained within the service remains the property of the NHS
The Data Protection Act 1998 and the Freedom of Information Act 2000 apply to email communication, this means that emails may have to be disclosed to individuals or outside agencies, as required by legislation or as required by any other statutory or legal duty imposed on the organisation
Guidance is given on the importance of proper email content including etiquette, structure, language and adding of attachments
The policy covers secure networks and transmitting over insecure networks including secure transfer of patient identifiable information

1. Introduction

This policy outlines the permissible use of business email when accessing Yorkshire Ambulance Service NHS Trust email services from the workplace or using network services remotely (e.g. when working on a laptop connected to the virtual private network or accessing work email via the internet). This policy additionally provides best practice guidelines aimed at making the most effective and secure use of the system for both internal and external email communications.

This policy applies to all employees of Yorkshire Ambulance Service NHS Trust (including contractors, bank, agency and temporary staff as well as volunteers) who use Yorkshire Ambulance Service NHS Trust network services to access the Trust's email system.

The Trust's email services include MS Exchange Server and Outlook as the main email system; however, other applications such as NHS Mail (Please see NHSmail Acceptable Use Policy), Clinical Hub, GRS, Cleric PTS and Adastra provide some email, messaging functionality and this policy and best practice guidelines apply equally to these and any other similar

communication systems used by the Trust. All data retained within the service remains the property of the NHS.

2. Purpose

Yorkshire Ambulance Service NHS Trust recognise that email is a necessary means of communication, a valuable resource and essential to support the business of the NHS.Email enables employees to communicate promptly and efficiently with other Employees, individuals and organisations.

The purpose of this policy is to ensure the proper use of email, so all employees are aware of what is deemed as acceptable and unacceptable use.

The provisions of the Data Protection Act 1998 and the Freedom of Information Act 2000 apply to email communication. This means that emails may have to be disclosed to individuals or outside agencies, as required by current Data Protection and Freedom of Information legislation or as required by any other statutory or legal duty imposed on the organisation.

3. Definitions

3.1 Defamatory Material

Published (spoken or written) material, which affects the reputation of a person or an organisation and exposes them to hatred, contempt, ridicule, being shunned or avoided, discredited in their trade, business, office or profession, or pecuniary loss.

3.2 Harassment

Any unwarranted behaviour, which is unreasonable, unwelcome or offensive. This may include comments or printed material, which causes the recipient to feel threatened, humiliated or patronised.

3.3 Copyright

A term used to describe the rights under law that people have to protect original work they have created.

3.4 Unsolicited

Not looked for or requested.

3.5 Pornography

The description or depiction of sexual acts or naked people that are designed to be sexually exciting.

3.6 Encryption

The process of transforming information (referred to as plain text) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.

3.7 Anonymised

Stripped of all personal identifiable information or presented as an aggregate.

3.8 Pseudonymised

Uses some personal identifiable information i.e. NHS Number but only with additional effort would anyone be able to identify full personal details from this information.

3.9 Chain Letter

One of a sequence of letters, each recipient in the sequence being requested to send copies to a specific number of other people

3.10 Junk Mail/SPAM

Unsolicited advertising or promotional material received through the mail or email.

4. Duties

4.1 Trust Management Group (TMG)

The Trust Management Group consists of Executive Directors and Associate Directors and is chaired by the Chief Executive. The Group carries delegated responsibility from the Trust Executive Group for approving this policy.

4.2 Document Owner and Document Lead

The Associate Director of ICT and Infrastructure, Development and Systems Manager are responsible for ensuring this policy is reviewed periodically and is in line with legislation, Department of Health requirements and best practice. The Document Owner and Document Lead are responsible for overseeing the implementation of this policy including monitoring compliance.

4.3 Line Managers

All line managers are responsible for ensuring that all employees are aware of this and related policies.

4.4 All Staff

All staff are responsible for making sure they have read and understood this policy and are aware of the disciplinary and legal action that could potentially be taken if this policy is not followed. All staff must exercise professional behaviour and etiquette when carrying out email communication on behalf of the Trust.

5. Email Acceptable Use and Management Processes

5.1 Prohibited Use

The use of email in the following types of activities is specifically prohibited;

- Creating or sending any offensive, pornographic, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.
- Creating or sending any messages that may constitute racial or sexual harassment.
- Creating or sending any material which is designed or likely to cause annoyance, inconvenience or needless anxiety.
- Creating or sending any defamatory material.
- Sending any material which may infringe on the copyright or licencing laws of another person or company.
- Sending any unsolicited commercial or advertising material to other users or organisations connected to other networks.
- Initiating or forwarding electronic chain letters, spam or junk mail.
- Sending email to randomly selected recipients including the use of bulk emails and excessive use of mailing lists, which is unrelated to the legitimate functions of the Trust and likely to cause offence or inconvenience to those receiving it.
- Forging or anonymously sending mail. All emails must be attributable to a named sender.
- Impersonation or misrepresentation of another individual.
- Sending email using another person's email account by using that individual's identity (i.e. the individual's username/password details).
- Undertaking any actions which are intended to use unreasonable system resources or otherwise interfere with other users ability to utilise the local network
- Knowingly sending an email or attachment that contains a computer virus or other harmful software
- Making any attempt to break into and / or access an email account which you have no legitimate right to use, either on Trust systems or any other sites.
- Making use of the mailing system for anything other than Trust business e.g. the use of private email for any commercial activity or monetary gain.
- Any use that could result in the inadvertent commitment of the Trust to a contract or agreement if it appears to the other party that he/she has authority to do so.
- Using external email accounts (e.g. Hotmail) for Trust purposes. This includes auto-forwarding of Trust email to external accounts. The only exception to this is NHS NET mail accounts.
- Using email for personal reasons to promote or denigrate companies or organisations, or defame other employees.
- Any use that violates Trusts policies, standards or procedures.
- Any use that brings the Trust into disrepute.
- Storing details in the Outlook electronic diary containing patient identifiable information. Electronic diaries are generally accessible by all members of staff.

Remember that emails are classified as "legal" documents and are admissible in court.

5.2 Best Practice

The Trust considers email to be an important means of communication and recognises the importance of proper email content and timely replies in conveying a professional image. The Trust therefore encourages staff to adhere to the following guidelines:

- Do not use email as a filing system. Attachments and emails that constitute a record should be transferred to an appropriate filing system.
- Write well-structured emails. Always use a brief, but descriptive, subject line for your messages. Some people will automatically delete messages which contain no subject.
- Be as brief as reasonably possible and avoid the use of digitised images (logos etc.), in order to minimise the amount of network traffic.
- Include your name, job title and the name of the Trust.
- Any email messages sent externally will carry the authority of the Trust. Users should maintain the same literary standards as those used on letter headed paper and the same degree of politeness.
- Only mark emails as important if they really are important.
- If you need a reply to your email by a particular date let the recipient know this.
- Use the spell checker before you send out an email.
- Proof read your messages before you send them, just as you would a paper document. Ensure you comply with the Trust's Style Guide.
- Before sending, check that the correct email address has been typed or chosen correctly. Messages can be addressed to the wrong person by mistake e.g. recipient with a similar name; automatic completion of an address by the Outlook email 'auto complete' functionality. Where possible select recipients names directly from the Outlook Global Address list.

- Once a message has been sent out, you can no longer change it and it may be stored in several places. Therefore you should carefully consider the content and language used in electronic messages.
- When replying to a specific message, remind the sender or other readers briefly of the point of the message to which you are responding.
- Keep in mind when you are sending messages, or responding to messages sent by others, that your readers may have different views, opinions and cultures. Email does not provide vocal inflection or body language, thus sarcasm, facetiousness and otherwise innocent "fun" can easily be misinterpreted as being rude or abusive (remember that if people are away they may have redirected their email to someone else). Words in capitals in email can be considered as shouting.
- Do not send messages or attachments unnecessarily. In addition to network traffic larger messages will require more storage space. Unnecessary messages may result in unnecessary costs to the Trust.
- If you have to send a large document to a number of different people it is far more efficient to keep it in a common network directory and send messages giving the location of the document (or hyperlink) rather than sending the document itself.
- When sending email across the NHS network users should zip or compress attached files (wherever possible) to help reduce network traffic. Wherever possible users should send external messages in excess of 150Kb as zipped

files. All users of the Trust network have the basic functionality as part of Microsoft Windows to compress files before sending them.

- Ensure that all unwanted messages are deleted.
- Electronic mail attachments may be a software program, executed when an attachment is opened. These programs may not be benign and may include computer viruses. The damage they cause may not always be immediately apparent. If in doubt seek advice from the ICT Service Desk before opening any attachment.
- The email software has a program which regularly checks for new messages and will report when one has arrived. It is tempting to automatically switch to the new email message, although the interrupted task may be of higher priority. Email messages are an alternative to paper post; as such they can be dealt with in a similar manner by allocating a specific time (perhaps morning and afternoon) for dealing with the electronic "post". To disable (or enable) the automatic notification please contact the ICT Service Desk.
- When forwarding messages, including a lengthy chain of past correspondence, you should carefully consider whether it is appropriate to send all the information to the new recipient list.
- It is possible for email to be read and sent (in the users name) from an unattended computer. It is the user's responsibility to ensure that whilst their computer is unattended access is restricted, either by logging out, switching the computer off or by locking the workstation using the CTRL ALT and DELETE keys.

5.3 Administration of Email Accounts

5.3.1 Opening and Closing Email Accounts

Email accounts for staff are set up by the ICT Service Desk on receipt of a request from department heads. Associated passwords are issued directly to the end user or via their line manager.

Staff accounts are deleted on receipt of a request from Human Resources. Following the departure of a member of staff from the Trust, their email account will be closed for access by them and then deleted after a period of 180 days.

5.3.2 Requests for Access to Email Communication

The Trust has an automatic centralised system to archive emails. This enables the tracking and retrieval of previous emails in respect of correspondence that would be significant in an internal or external matter (e.g. correspondence of a contractual nature). Request for access to email communication must come from a Director or Associate Director and must be authorised by the Associate Director of ICT (or appropriate deputy).

The Trust reserves the right to enable 3rd party access to email accounts in exceptional circumstances e.g. to make arrangements to cover long term sickness leave or for personal emergencies where absence from work is

unexpected. Where there is an immediate business need to have access to this information the following steps should be followed:

- Email authorisation from the employee's Associate Director to the ICT Service Desk is required. This should name the staff member requiring access, and the expected duration.
- Based on business need, the email from the Associate Director should state if access to the Inbox is required, or the entire Mailbox, including Sent Items and sub folders.
- The staff member should be informed of the access, business justification, the nominated individual who had access, and the period of time.
- Any emails marked as 'Private' or 'Personal' in the subject heading must not be read, as the purpose of the above is to access business information.

5.3.3 Delegated Access

Staff may delegate rights to other email users by modifying their own Outlook user profile information. This will allow other staff to have different levels of access to their Outlook email, calendars etc. Staff remain responsible for granting access permissions and ensuring these are only granted in appropriate circumstances.

5.3.4 Email Account Retention

Emails will be retained until a member of staff leaves the Trust. At this point their email will be retained for a further 180 days.

5.3.5 Housekeeping and Archiving

Email capacity is not unlimited. Staff should regularly delete unwanted emails from their Inbox (including sub folders) and Sent Items. Once this is done, staff should remember to empty their Deleted Items folder.

If you receive an email from the ICT 'System Administrator' you will need to to attachments) and not number of emails that will fill up the quota. If you genuinely need to retain old emails for business reasons, then you should move these to an Outlook personal folder or transfer them to an appropriate network filing system such as the 'I' drive.

5.4 Acceptable Personal Use

Email is primarily for business use. The use of email for occasional and reasonable personal use is permitted, subject to the terms of this policy. Personal use must not directly or indirectly interfere with the Trust's systems or burden it with any costs.

Personal emails should be kept in a separate folder, named 'Private'. The emails in this folder must be deleted regularly. In appropriate circumstances where the Trust feels that this policy has not been complied with, the Trust

may look at this folder.

Requests for access must come from a Director or Associate Director and must be authorised by the Associate Director of ICT (or appropriate deputy).

The Trust reserves the right to manage a mailbox on behalf of an individual (see section 5.3.2).

5.5 Email and Working Remotely

Access to the Trust's email systems for staff is available remotely (e.g. blackberry device, using a Trust supported laptop with remote access or via Outlook on the Web). Remote access is at all times subject to the terms of this policy.

Staff must not download Trust related emails or attachments onto a computer or other device which is not supported and managed by Yorkshire Ambulance Service NHS Trust.

5.6 Out of Office Assistant

If you are going to be out of the office you should turn on your 'Out Of Office'. When this is turned on it will automatically reply with a given message to anybody that sends you an email. The 'Out Of Office' message should state when you will be able to reply to the message and alternative contact details for colleagues that may be able to assist. Colleagues listed in an out of office assistant message should be made aware of this prior to this being enabled.

5.7 Email Disclaimer

The use of email disclaimers are recognised as good practice, though not legally binding. All outgoing email (external to the Trust) is automatically marked with a disclaimer message as set out below. This must not be edited or deleted.

Emails and any attachments from Yorkshire Ambulance Service NHS Trust are confidential. If you are not the intended recipient, please notify the sender immediately by replying to the email, and then delete it without making copies or using it in any other way.

Any views or opinions presented are solely those of the sender and do not necessarily represent those of Yorkshire Ambulance Service NHS Trust unless otherwise specifically stated.

Although any attachments to the message will have been checked for viruses before transmission, you are urged to carry out your own virus check before opening attachments, since Yorkshire Ambulance Service NHS Trust accepts no responsibility for loss or damage caused by software viruses.

Senders and recipients of email should be aware that, under the Data Protection Act 1998 and the Freedom of Information Act 2000, the contents may have to be disclosed in response to a request.

5.8 Personal Information, Sensitive Personal Information and Commercially Sensitive Information

Personal data is information about living individuals that can be used on its own or with other information to identify an individual or individuals. It includes for example, name, address, date of birth, postcode, national insurance number which together, individually or in combination with other information could allow a person to be identified. It can include for example information about individual's salaries, performance development reviews and references.

Sensitive personal data covers personal identifiable information which specifically contains details of an individual's:

- Health or physical condition e.g. all patient identifiable information which the Trust processes, staff occupational health referrals and reports
- Sexuality/sexual life
- Ethnic origin
- Religious beliefs
- Trade union membership
- Political opinions
- Criminal convictions

The Data Protection Act 1998 defines both personal data and sensitive personal data.

Commercially sensitive information may for example relate to information whose disclosure could prejudice the conduct or outcome of contractual or other negotiations.

Where email has been agreed as the most appropriate method of transfer of personal information, sensitive personal information or commercially sensitive information then the following security **must** apply.

5.8.1 Emails sent within the Trust's secure network i.e. from a YAS to a YAS email account (…….@yas.nhs.uk)

The minimum amount of information should be sent.

Where the correspondence relates to more than 4 identifiable individuals the information must be sent in a password protected file attachment. The password must be relayed to the recipient via a person to person phone call.

All staff are responsible for maintaining the confidentiality of information and complying with the Caldicott Principles and the Data Protection Act 1998.

Factors that will influence whether email is a suitable approach (or whether an

alternative approach is advised, such as transferring the information via 'shared drive') include:-

- the type of information
- its intended use
- intended frequency of transfer
- the intended recipient(s)

5.8.2 **Emails sent outside of the Trust secure email network**

Emails must only be transmitted to recipients outside of the Trust's secure email network by using one of the three methods detailed below:-

- By use of NHS Mail (both the sender and the recipient of the email MUST be using NHS mail email addresses). NHS Mail is also widely known as NHS.net email. See 5.8.3 below.
- By encryption (to 256 bit AES) of the information within a strongly password protected file attached to the email correspondence. The Trust supports the use of WinZip for file encryption. Staff should contact the ICT Service Desk in relation to access to WinZip.
- By Secure File Transfer Protocol (SFTP)

Strong passwords must be eight characters, alpha numeric, mixed upper and lower case.

All transfers of person identifiable information, sensitive person identifiable information and commercially sensitive information outside of the Trust's secure email network must be authorised by a Departmental Information Asset Owner or Head of Department.

5.8.3 **NHS Mail**

NHS Mail is the brand name for nhs.net email. NHS.net is a secure national email service which enables secure exchange of sensitive and patient identifiable information within the NHS and with local / central government. All user connections to the service are encrypted, this removes the need to separately encrypt or password protect attachments.

NHS.net is the only Department of Health approved email service for the secure exchange of clinical data between NHS organisations and the government email domains below:

The recipient's email address must be either nhs.net or one of the listed secure government domains.

Central Gov
x.gsi.gov.uk
.gsi.gov.uk
.gse.gov.uk
.gsx.gov.uk
.police.uk
.pnn.police.uk

.cjsm.net
.scn.gov.uk
.mod.uk

Local Gov
.gcsx.gov.uk

5.8.4 Further Considerations

The following should be considered before sending any person identifiable information, sensitive person identifiable information or commercially sensitive information by email:

- Ask yourself if it is absolutely necessary to send via email
- Only send such information on a "need to know" basis
- Ensure person identifiable information is kept to a minimum
- Never use web based systems e.g. Hotmail or Yahoo
- Only use methods described in this section

Consideration should also be given as to whether the data can be anonymised when transmitted by email. If the data cannot be anonymised, consideration should be given as to whether it can be pseudonymised i.e. using NHS number or a recognised internal number as the only identifier. Anonymised information can be sent using the email system without approval.

Never put patient safety at risk. If in doubt as to whether it is clinically justifiable to anonymise / pseudonymise the information, speak with your line manager in the first instance.

5.8.5 Recording New Transfers of Person Identifiable Information

Where a transfer of person identifiable or sensitive person identifiable information by email is a 'new' transfer (flow) staff must contact their Information Asset Owner or the Information Governance Manager so that the data flow can be recorded.

5.8.6 Personal Responsibility

All staff are personally responsible for correctly addressing and for sending person identifiable information, sensitive person identifiable information and commercially sensitive information in a secure manner by email.

Staff should always seek advice via the ICT Service Desk if in any d
oubt about the security of an intended email transmission.

5.9 Auditing and Monitoring

The email system is the property of Yorkshire Ambulance Service NHS Trust.

The Trust does not routinely monitor or access the content of email. However, all emails are automatically scanned for viruses and for “spam” content i.e. whether they match unsolicited, nuisance, emails previously sent to the Trust: all such emails are blocked. However, filtering/virus-scanning can never be 100% effective so any unsolicited emails and attachments should always be treated with caution. Similarly, an email may be incorrectly marked as infected or “spam” and become unnecessarily blocked.

Under UK law, employers are generally liable for what their employees do in the course of their work. This includes employees using email to send defamatory or offensive messages. The Trust therefore reserves the right of access to users’ email and audit logs on both the client workstation as well as the servers for legitimate purposes, such as investigation of complaints of misuse. Contents and audit logs for both sent and received email may be inspected (including personal email) at any time without notice. Authorisation has to be given by the Associate Director of ICT (or appropriate deputy) for access to staff email.

If the finding from a specific monitoring exercise necessitates the need to refer to an external agency such as the Police, then the Trust will do so as soon as practically possible.

ICT reserves the right to take special actions in administering email if this is essential to preserve the integrity or functionality of the system.

6. Consultation Process

Members of the Information Governance Working Group have been included in the development, consultation and review of drafts for this policy.

7. Approval Process

This policy has been reviewed by Information Governance Working Group members and approved by the Senior Management Group.

8. Dissemination and Implementation

Following approval, this policy will be made available to all staff via the Trust’s Intranet. The approval of this policy will be communicated to staff via the Trusts’ weekly Operational Update publication and by the use of NetConsent. The Policy will be communicated to staff at Corporate Induction and as part of the mandatory information governance training programme.

Everyone who is provided with access to Trust email is personally responsible for making themselves aware of and complying with this policy.

9. Monitoring Compliance

All staff (including contractors, temporary, bank, agency staff and volunteers) must adhere to this policy and comply with applicable UK legislation and any regulatory requirements for information governance. Failure to follow this policy and related information governance policy and procedures may lead to disciplinary, criminal or civil action being taken against the staff member. In the event of an agency worker or casual worker failing to comply with this policy and related policy and procedure, his / her work with the organisation may be terminated. The contract may also be terminated if the employee is an employee of a contractor.

A variety of methods will be used for monitoring email policy compliance including:

- Review of data flows to ensure confidential information is being transferred securely.
- Quarterly information asset owner risk reviews.
- Regular audit of information governance processes undertaken in line with policies and procedures in key areas i.e. confidentiality, data protection, information security, freedom of information.

10. Monitoring Effectiveness

To be assured that this policy is being implemented, key elements will be monitored for compliance.

Minimum Requirements	Monitoring
Statistically validated reduction in Information Governance related incidents (relating to insecure data transfers by email).	Monitoring of incidents by both the Clinical Governance Group (Caldicott Log) and through the Information Governance Working Group.
No Data Protection Act undertakings, enforcement notices or 'stop now' orders, compulsory assessment notices or monetary penalty notices served on the organisation. No Freedom of Information Act enforcement notices served on the organisation.	The Trust Board will monitor progress via the Integrated Performance Report and the Quality Committee will monitor progress through receipt of quarterly Information Governance reports.
All staff receive annual training and competency test in information governance.	The Trust Board will monitor progress via the Integrated Performance Report and the Quality Committee will monitor progress through receipt of quarterly Information Governance reports.

11. Associated Documentation

The following is a guide and is not exhaustive:

- Internet Policy
- ICT Security Policy
- Data Protection Policy
- Information Governance Policy
- Information Governance Strategy
- Information Risk Procedure
- Records Management Policy
- YAS Code of Conduct
- Disciplinary Policy and Procedure
- Bullying and Harassment Policy and Procedure
- Freedom of Information Procedures
- Management of Procedural Documents Policy
- Style Guide
- NHS Mail Acceptable Use Policy

12. References

12.1 Legislation

- Great Britain. 1998. *Data Protection Act 1998*. London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 2000. Freedom of Information Act 2000. London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 2004. *Environmental Information Regulations 2004.* London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 1990. *Computer Misuse Act 1990. Chapter*. London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 1990. *Access to Health Records Act 1990. Chapter*. London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 1958 and 1967. *Public Records Act 1958 and 1967.* London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 1998. *Crime and Disorder Act 1998*. *Chapter*. London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 2000. *Electronic Communications Act 2000.* London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 1998. *Human Rights Act 1998*. London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 2000. *The Regulation of investigatory Powers Act 2000.* London: HMSO. Available at: www.legislation.gov.uk

12.2 Guidance from Other Organisations

- NHS Connecting for Health. Publications: Information Governance Toolkit. Available at: www.igt.connectingforhealth.nhs.uk
- Letter from the Chief Executive of the NHS in England, Publications: Department of Health Gateway Reference 9185. Available at: www.connectingforhealth.nhs.uk