Electronic Communications

Version Number	2	Version Date	18 Aug 2013
Policy Owner	Chief Finance and Commercial Officer		
Author	IG Lead		
First approval or date last reviewed	July 2011		
Staff/Groups Consulted	Information Governance Steering Group Policy Group		
Discussed by Policy Group	19 March 2013		
Approved by HMT	27 March 2013		
Next Review Due	31/03/2016		
Equality Impact Assessment Completed	March 2013		

Table of Contents

1. RATIONALE

Yeovil District Hospital Foundation Trust recognises that electronic communications are a valuable and essential resource in allowing employees, individuals and organisations to communicate effectively and efficiently.

2. POLICY STATEMENT

The Trust encourages the use of electronic rather than paper communications wherever possible. The objective of this policy is to ensure that staff make best use of electronic communication systems, whilst maintaining the Trust's security and legality, avoiding misuse, protecting individual staff as well as maintaining the Trust's professional image.

3. APPLICABILITY

This policy applies to:

- all Trust employees whilst engaged in work for the Trust at any location, using any form of electronic communication systems and devices including remote access
- any other use by Trust employees which identifies the person as a Trust employee or which could bring the Trust into disrepute using any form of electronic communication systems and devices.
- other persons working for the Trust, persons engaged on Trust business or persons using Trust equipment and networks
- all usage by anyone granted access to the Trust networks, media, devices including remote access
- any persons using Trust networks, systems, devices for personal electronic communications

Failure to follow this policy by staff may result in action under either the Disciplinary or Capability policies. Other persons may be subject to other action by the Trust.

4. POLICY PROVISIONS

Legal Requirements

Electronic communications systems are tools that users are obliged to use in a responsible, effective and lawful manner. Although some communication systems can seem less formal than written communication, the same laws apply. It is therefore important that users are aware of legal risks.

You and the Trust can be held liable if Communications:

- Are forged or forgery is attempted
- Are sent using another person's account
- Are forwarded with any libellous, defamatory, offensive, harassing, racist, obscene or pornographic remarks or depictions

- Containing confidential information are unlawfully forwarded with an attachment that contains a virus
- Are in breach of the copyright or licensing laws when being composed or forwarded

Personal Use

Although the Trust communication systems are primarily for business use, the reasonable, moderate use of these systems for personal use is permitted in line with Trust policies, protocols and procedures.

Sensitive Personal Information

Sensitive personal information (ie that relating to identifiable individuals) or commercially sensitive information must not be sent externally by email unless it is encrypted to NHS standards using software approved by the Trust. YDH has arrangements in place to send encrypted email messages to all other NHS Organisations in Somerset using a secure process.

NHSmail encrypts data between NHSmail accounts to standards approved by the NHS, therefore, it can be used for sending sensitive personal information.

All messages sent outside of the County and to non NHSmail addresses must be encrypted by using the word ENCRYPT in the message subject header. This will ensure the message cannot be intercepted.

System Monitoring

All systems are monitored for viruses. All email traffic (incoming and outgoing) is logged automatically. The logs do not include email content. These logs are audited periodically.

The content of emails is not routinely monitored. However, the Trust reserves the right to retain message content as required to meet legal and statutory obligations.

The Trust monitors internet usage, including the use of blogging sites, YouTube and social network sites.

Freedom of Information Act 2000

Communications, whether sent internally, or externally should be regarded as public and permanent. Content of a business nature may be liable to disclosure under the Freedom of Information Act. Care should be taken in composing communication to ensure only material relevant to the topic is included. Communications ie emails deleted from drives but remaining on servers can be requested.

5. ASSOCIATED PROCEDURES

Appropriate guidance to support this policy will be agreed by the Information Governance Steering Group and published for all staff to access via the Policies Database

- YDH Email Etiquette and Guidance
- YDH Social Media Guidance
- YDH Web Browsing Guidance

6. IMPLEMENTATION, MONITORING AND EVALUATION

6.1. Following approval by the Trust Policy Group and Board of Directors this Policy will be held on the Trusts Policy Database. It will be publicised in the weekly brief and made reference to at Trust Induction and Mandatory training sessions.

6.2. Appropriate guidance, processes and procedures will be embedded in IT system users training sessions

6.3. The effectiveness of this policy will be monitored by the Information Governance Steering Group.

- Somerset Health Informatics will report to the Data Protection Officer, IG Lead and Caldicott Guardian any breaches of security or misuse of electronic systems highlighted through system monitoring or reporting

- Where an IG incident arises that breaches this policy an incident form will be completed and reviewed by the Data Protection Officer, IG Lead and Caldicott Guardian. This will then be discussed at the IG steering group meeting.

6.4. This policy will be evaluated and updated in line with any actions or improvements required as a result of monitoring outcomes, also as directed by any local and national guidance. These changes will be reviewed by the Information Governance steering group, Trust Policy Group and Board of Directors before implementing and updating staff.

7. DEFINITIONS

- **Electronic Communication** is the process of communicating via an electronic system/device

8. TABLE OF ROLES AND RESPONSIBILITIES

Chief Executive	• Has ultimate responsibility for ensuring the Trust has suitable arrangements in place for the management of electronic communications
Board of Directors	• Responsible for taking appropriate action regarding any breaches of the electronic communications policy
Chief Finance and Commercial Officer	• Responsible for taking appropriate actions and reporting any breach of the Electronic Communications Policy directly to the Board of Directors
Line Managers	• Promote a culture that encourages staff to use electronic communication systems appropriately and ensure staff adhere to the policy
Taunton & Somerset IT Services	• Ensure that electronic communication systems are available to users • Preserve Integrity by protecting the

	systems from unauthorised or accidental modification ensuring the accuracy and completeness of the Trust's assets. • Preserve Confidentiality by protecting assets against unauthorised disclosure. • Ensure that all users are properly trained before using electronic systems
IG Steering Group	• Responsible for agreeing and issuing any changes to the electronic communication policy, protocols, procedures and legal obligations.. • Review any breaches of this policy
IG Lead	• Responsible for updating and disseminating any changes to policy, protocols, procedures, legal obligations. • Deliver training to all staff attending Trust induction and mandatory training programme.
All staff	• must be aware of and abide by policies, protocols, procedures and legal obligations relating to the use, of electronic communications. • Attend staff Induction and mandatory training programmes.

9. REFERENCE TO OTHER POLICIES

Users are responsible for making themselves aware of other associated Trust policies:

- Information Governance Policy
- Information Security Policy
- Records Management Policy
- Data Protection Policy
- Disciplinary Policy

10. SOURCE REFERENCES AND ACKNOWLEDGEMENTS

- Copyright Designs and Patents Act 1988
- Computer Misuse Act 1990
- Caldicott Report 1997
- The Data Protection Act 1998
- The Data Protection Act 1998 (Employers Code of Practice)
- The Human Rights Act 1998
- Electronic Communications Act 2000
- Regulation of Investigatory Powers Act 2000
- NHS Confidentiality Code of Practice 2003
- Records Management NHS Code of Practice 2006
- NHS Information Security Management of Practice 2007
- Obscene Publications Act 1959

ANNEX A – EQUALITY IMPACT ASSESSMENT TOOL

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

		Yes / No / N/A	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	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?	N/A	
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 the Trust's lead for Equality & Diversity, 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 the Trust's lead for Equality & Diversity.

Signed – Name: Karen Carter Date: 18 March 2013