Camden and Islington NHS
Mental Health and Social Care Trust

Internet and E-Mail Policy

Version 2.1

Camden *supporting partnership in mental health* ISLINGTON

This policy has been created in order to provide framework and guidance for staff and the Care Trust to manage the Internet and Email Business Tools. The framework provided accounts for the variety of IT suppliers across the Care Trust by holding management responsible for staff usage of the Business Tools. The policy provides an overarching structure to support local implementation across all Care Trust sites.
The policy was developed after a literature review and a current analysis done by the development group. The first drafts will be circulated amongst the development group for a first revision. The agreed draft policy is to be then returned to the Care Trust Board for Information Systems Strategy (the body requesting the policy) for review and publication.

Group Membership	
Barry Duke	Information Manager
Stephen Greenhalgh	Systems and National Programme Manager
Timothy d'Estrubé	Information Governance Manager

Consultation Framework

IWL Workgroup

Directorate dissemination

Care Trust Board for Information Systems Strategy (BISS)

Ratified by Care Trust Board for Information Systems Strategy (BISS)

Signature …….Chief Executive/Chair of BISS

Date:

Audit:

Review Date:

Version Control

Version	Author(s)	Revision Date
1.0	Timothy d'Estrubé – Information Governance Manager	Jan 05
2.0	Timothy d'Estrubé – Information Governance Manager	

Version	Board Approved	Approval Date	Replacement Date
1.0	Draft	~	~
2.0	Approved	March 16th 2005	Pending
2.1	Pending		

Table of Contents

Internet and Email Policy

1 Aim of Guidelines/Policy

This policy provides the boundaries in which the Internet and Email Business Tools of the Care Trust are to be used.
Rather than attempting to place the responsibility on the Care Trust's IT systems and suppliers, this policy enables and encourages responsible management of Care Trust staff within the Care Trust management structure. In this way the risk of fallible technology and accidental or intentional misuse of these business tools is reduced.
This policy retains the emphasis on Care Trust staff responsibly using the business tools to further the business and interests of the Care Trust, but allows for the flexibility and compassion to provide the Care Trust's communication technology for responsible personal use.
This policy is intended to:

- Provide principles and expectations of the Care Trust and the greater public for Care Trust staff to uphold when using the Internet or Email Business Tools
- Provide guidance to staff on how to assess the appropriateness of their usage of these business tools
- Provide specific examples of misuse
- Provide a platform which is compliant with privacy and confidentiality laws that the Care Trust can use to take action against misuse
- Enforce practices that protect the Care Trust, its staff and its service users
- Establish clear lines of management responsibility in regards to the use of these tools

2 Introduction/ Background

The advent of the Internet has provided an equally powerful, flexible and long-ranged method of communication. The Care Trust provides Internet browsing and Email tools to its staff in order to gain the advantages of this method of communication, but it does so at considerable financial cost and risks to its reputation and trust of the public. The Care Trust recognises that its employees will be generally responsible but, human nature being what it is, there is a potential for distraction and accidental or intentional misuse of these business tools. In order to manage the risk of distraction to its staff, or misuse of the tools by staff, the Care Trust has provided this policy. This policy serves as guidance for proper use, discouragement for misuse and protection of the rights of the Care

Trust to maintain its business and interests in balance with staff members' and the publics' right to have their privacy and confidentiality respected.

This policy draws from a variety of sources, although is primarily developed from the statutory requirements of the:

- Data Protection Act 1998

As well as guidance from:

- Internet & E-Mail Usage Policies and Procedures (Islington PCT, ICT Shared Services, V 1.04f)
- The Employment Practices Data Protection Code; Part 3: Monitoring at Work (Information Commissioner, V1.0)*
- The Employment Practices Data Protection Code; Part 3: Monitoring at Work: Supplemental Guidance (Information Commissioner, V1.0)*
- Guidelines on developing a policy for managing email (The National Archives, First Version 2004)

* Contains guidance on Lawful Business Practice Regulations 2000 and Investigatory Powers Act 2000

3 Usage of this policy

This policy is not intended for every-day front line usage. What this policy does is set the overall framework for the usage and management of the Care Trust's Internet and Email Business Tools. This provides the basis for front line documents, such as codes of conducts and protocols as well as a platform from which further sub-policies may be based. This policy is designed such that it would be a companion or child document to an overall IT policy.
Note that throughout this policy where reference is made to this policy (for compliance or other purposes) appropriate child documents of this policy may be substituted. For instance; reference to staff having read and understood this policy would be understood as staff having read and understood the code of conduct based on this policy.

4 Guideline /Policy statements

4.1 Policy Principles & Framework

This section outlines the general principles the framework for the Care Trust's use of the Internet and Email Policy is based on.

4.1.1 Principles Introduction

The Care Trust provides two states of usage for the Internet and Email Business Tools. The basic state of usage is for business purposes only, and is espoused in principles one and two. The second state of usage provides reasonable personal usage of the Internet and Email Business Tools, and is espoused by principle three. Principle four ensures that the Care Trust has a responsibility to its staff to provide this policy and any other relevant guidance so that they are well informed and educated on the correct usage of the business tools. Full definitions of the principles can be found in Appendix Six – Business Tool's Policy Principles

4.1.2 Framework

This policy sets up a responsibility framework based on the line management structures of the Care Trust. Line Management is responsible for both granting

	Introduction	the privilege of personal usage to staff as well as taking proactive measures to ensure that the business tools are not being abused or misused. This approach mitigates the risks of relying on fallible technology and being dependent upon multiple suppliers for our email and network services. It does however open risks to staff and Care Trust alike if incorrect, abuse or unjustified invasion of privacy occurs as part of the proactive measures, or the opposite where-in no proactive measures are taken and abuse of the business tools occurs un-detected as a result. Ultimately the best approach is mixture of technological and managerial approaches to managing tools such as the Internet and Email. While this policy emphasises the human component through the management structures of the Care Trust it does not exclude the use of technology as a supporting tool.
4.1.3	Principle 1	The Care Trust will not tolerate use of IT, network and email systems that is not directly related to Care Trust interest or business. (See Appendix Six - Policy Principles for the full principle)
4.1.4	Principle 2	The Internet and Email Business Tools are the property of the Care Trust and any material produced or received via these tools are either under the ownership or custodianship of the Care Trust. Individuals may not claim personal ownership or custodianship of any material transferred to or created on the network or e-mail system regardless of subject matter, and hence should be aware that there is no absolute guarantee of privacy or confidentiality while such material exists on the Care Trust's network. (See Appendix Six - Policy Principles for the full principle)
4.1.5	Principle 3	The Care Trust may extend a privilege to staff to use the Care Trust's business tools for personal use under appropriate and limited circumstances. This privilege would require staff to respect the boundaries in which the privilege is given and would be provided on the continual respect of those boundaries and business circumstances of the Care Trust (See Appendix Six - Policy Principles for the full principle)
4.1.6	Principle 4	The Care Trust will provide policy and guidance to its staff so that they are made aware of what constitutes acceptable usage of these business tools, the penalties for misuse, the limitations of any privileges granted and the reasons and ways in which monitoring may take place. (This is the full principle as found in Appendix Six - Policy Principles). The Care Trust responsibilities regarding Principle 4 is defined in section Appendix Three – Executive and Corporate Responsibilities
4.1.7	Principle 3 vs. Principle 1	When granting the privilege of personal usage the Care Trust is relaxing the first principle of this policy to allow for sanctioned use of Internet and Email business tools for limited and respectful personal use. Effectively Principle 1 and Principle 3 are the opposites ends of the spectrum of usage allowed by the Care Trust. Principle 1 is the complete business use of the Internet and Email business tools while at the opposite end of this spectrum is Principle 3, the limited and respectful personal usage of the business tools. Staff members will use the business tools under either Principle 1 or Principle 3 at any given time. Note that Principle 3 does not allow staff's personal use to come into conflict

with the interest or business Care Trust, and any such conflicting action by staff will result minimally in the revocation of the privilege, and for more serious incidents application of this policy as though the privilege had not been granted.

4.1.8 Principle 3 vs. Specific Misuse

The granting of the privilege does not negate those items listed as specific misuse listed in Appendix Five - Appropriate Usage Guidance and Mis-Usage. As the privilege does not negate these items or the power this policy has in regards to those items, staff should not expect to have any protection under the privilege of personal usage if misusing the Internet or Email.

4.2 How the privilege of Personal Usage is granted

The privilege of personal usage is granted through the line management hierarchy. Beginning with the Chief Executive, each successive level of line management grants the next level the privilege of using the Internet and Email business tools for personal use. So for instance; Directors grant their directorates the privilege, Services Managers within the directorate grant their services the privilege through the Local Managers, Local Managers grant their Team Managers, and Team Managers their staff. The privilege is encouraged to be common across the Care Trust, however each level of the hierarchy can apply the privilege as they see fit. Should a particular service or team have limited computers on which to work it may be wise to grant limited or no personal use until the resources can comfortably allow the luxury of personal usage. Further guidance on the granting of personal privilege can be found in Appendix Two – Management Responsibilities and Guidance

4.2.1 Line Management Responsibility vs. Technological Responsibility

Because of the structure of the privilege approval all line managers will be responsible for the staff beneath them. Therefore it is expected that managers take reasonable and active steps, in tandem with any technological and/or automated safeguards available, to ensure that the staff under their supervision are complying with this policy. Failure to do so on the part of line management will endanger the Care Trust and the staff involved. The Care Trust therefore may enact disciplinary or dismissal procedures upon line management, even in cases where no harm has come to the Care Trust, should it find that said line management are negligent, complacent or unwilling to enforce this policy with their staff.
For further guidance on the on line management responsibility please see Appendix Two – Management Responsibilities and Guidance.

4.2.2 Where staff dispute the privilege granted to them

Where staff feel that they are unfairly being denied personal usage privilege they are encouraged to speak to their line managers. If the situation cannot be resolved through speaking with their line manager parties are encouraged to request a decision to be made at the next highest and appropriate level of senior management. Staff are also encouraged to speak to their appropriate staff and trade representatives.
Staff should remember however that the business tools are a continuous cost and risk to the Care Trust and as such personal usage will only be granted where the Care Trust feels it will not be compromising its business or interests. (See Appendix Six - Policy Principles for Principle 3)

4.3 Introduction to

Because of the flexibility and evolving nature of culture and technology it

Guidance Questions

would not be practical to list every situation that could qualify as misuse of the Care Trust's Internet and Email systems. Therefore the Care Trust has provided guidance in the form of questions that staff may ask of themselves when using the Care Trust's Internet and Email. Justifying usage according to these guiding questions will provide flexibility within this policy for unusual but appropriate usage as well as allow the opportunity for dialogue with the Care Trust about what constitutes appropriate usage. The questions change if the individual has been granted privileges to use the Internet or Email for personal use.
In addition to using the guidance questions below, all staff should follow the requirements and guidance outlined in Appendix One – All Staff Responsibilities and Guidance

4.3.1 Definition of a Reasonable Person

This policy depends on the "reasonable person principle". The reasonable person is a summation, or average of societal opinions and knowledge. Because of the impossibly objective nature of the Reasonable Person, it is expected that appropriate use of the Internet and Email will generate some discussion between staff and their line management. Further explanation of the reasonable person can be found in Appendix Five – Appropriate Usage Guidance and Mis-usage.

4.3.2 When the Care Trust disagrees with the staff member on what constitutes appropriate usage

The Care Trust has the ultimate responsibility for the users of its Internet and Email systems, therefore has the ultimate say in what constitutes appropriate usage or the decision of the "reasonable person". In practicality this means that line managers have both direct responsibility for their staff's usage of the Internet and Email and the definitive decision on what constitutes appropriate usage. Where staff and their line managers disagree over the definition of appropriate usage or the "reasonable person", either party may request a decision to be made, or guidance provided, at the next appropriate level of senior management.
It should be noted that line management does not have discretion to define appropriate usage, only to interpret what the Care Trust has defined as appropriate usage. Further guidance on what the Care Trust believes to be appropriate usage can be found in Appendix Five - Appropriate Usage Guidance and Mis-usage.

4.4 Questions for when no privilege for personal usage has been given

This section gives the guidance questions for use of the Internet and Email when the privilege of personal usage has **not** been granted. Staff that can provide the indicated answers when reviewing their usage of the Internet or Email via these questions will likely be using the business tools appropriately. These questions must be answered using the Reasonable Person principle as indicated above. Summaries of the guidance questions are given below.

4.4.1 Question 1

"Am I using the Internet or writing this email in pursuance of my duties as a Care Trust employee?"
To which the answer must be **YES**
(See Appendix Five for the further guidance on this question)

4.4.2 Question 2

"If a reasonable member of the public were to be watching over my shoulder, would they object or question my accessing the Internet or writing of this email?"

To which the answer must be **NO**
(See Appendix Five for the full question and further guidance)

4.4.3 Question 3

"If a reasonable member of the public were to review my writings or actions on the Internet or Email, would they be able to reasonably assume that I was acting or writing in a professional way and am a member of a respectable and professional organisation?"
To which the answer must be **YES**
(See Appendix Five for the full question and further guidance)

4.5 Questions for when the privilege for personal usage has been given.

This section gives the guidance questions for use of the Internet and Email when the privilege of personal usage **has** been granted. Staff will replace the first question set above with the questions below when they are using the Internet or Email for personal use and have been granted permission by their manager for this use. Staff that can provide the indicated answers when reviewing their usage of the Internet or Email via these questions will likely be using the business tools appropriately. These questions must be answered using the Reasonable Person principle as indicated above. Summaries of the guidance questions are given below.

4.5.1 Appropriate Usage under the Privilege Question 1

"If my activities using the Care Trust's Internet and/or Email were known to a reasonable member of the public, would they have cause to question or disagree with my activities or writings?"
To which the answer must be **NO**
(See Appendix Five for the full question and further guidance)

4.5.2 Appropriate Usage under the Privilege Question 2

"Through my use of the Internet or Email, would the Care Trust's resources, reputation and professionalism, business and interest and/or staff (including myself) be at risk?"
To which the answer must be **NO**
(See Appendix Five for the full question and further guidance)

4.6 Responsibilities of Staff

Depending on the level of the Care Trust line management hierarchy Care Trust staff will have different responsibilities.

4.6.1 General Responsibilities of all Staff

In addition to the guidance found in Appendix Five – Appropriate Usage Guidance and Mis-usage all staff are expected to follow the requirements outlined in Appendix One – All Staff Responsibilities and Guidance. In summary the requirements when not using Email or Internet for personal usage include:

- Clearly Identifying oneself
- Only expressing opinions fitting to an employee of the Care Trust
- Not communicating on behalf of the Care Trust unless authorised to do so.
- Not forwarding junk or "spam" emails

And when using the business tools for personal use, staff are also expected to follow these requirements, in addition to the ones above, in summary:

- Not to print personal materials on Care Trust paper
- Limit the size of email attachments

Staff Are further expected to understand the material in Appendix Seven –

Good Practice Guidance.

4.6.2 Responsibilities for Staff in a position of managing other Staff

In addition to having the responsibilities for usage of the Internet or Email business tools, as summarised above, staff in a line management position have the further responsibilities as found in Appendix Two – Management Responsibilities and Guidance. In summary these are:

- Appropriately provide the Personal Usage Privilege without prejudice or bias, and judge the granting of this Privilege on the basis of minimal risk to the Care Trust's time, resources and reputation and the competency of the staff on the Business Tools
- To proactively manage the privilege and risks to the Care Trust when providing the Business Tools
- Ensure this policy is communicated, understood and represented within their team(s) and service(s) and that sufficient training has been provided in this policy's use.
- Request any monitoring activity
- Monitor compliance to this policy for their team(s) and service(s)
- Ensure that disciplinary and dismissal procedures under this policy or in relation to this policy, are carried out fairly
- Authorise the granting of the Personal Usage Privilege within their team(s) and service(s)
- Ensure that they and their staff have signed any relevant declarations relating to the use of the Internet and Email policy. These declarations can be found under Appendix Three – Executive and Corporate Responsibilities

4.6.3 Responsibilities for Staff in a executive or corporate positions

In addition to the two sections above, staff of the Care Trust with executive responsibilities or are responsible for a corporate service have further responsibilities regarding the use of the Internet and Email business tools. These responsibilities are found in full in Appendix Three – Executive and Corporate Responsibilities. In summary these responsibilities are:

- Ensure this policy is communicated, understood and represented within their directorate(s) and/or services
- Provide sufficient training and resources to their directorate(s) and/or corporate services on this policy and the business tools themselves
- Monitor compliance to this policy for their directorate(s) and corporate service(s)
- Ensure through good practice that the public's and Care Trust staff members' privacy is not unnecessarily violated
- Authorise any monitoring activity or other legitimate invasion of privacy for the business tools (See Appendix Eight – Monitoring Responsibilities and Guidance for responsibilities and guidance)
- Ensure that disciplinary and dismissal procedures under this policy or in relation to this policy, are carried out fairly
- Authorise the granting of the Personal Usage Privilege within the Care Trust and/or directorates or corporate services

There are further corporate responsibilities for the Care Trust regarding its IT infrastructure and agreements with suppliers. Not all executive or corporate service staff will have these responsibilities however. The responsibilities can

be found here in full Appendix Four – IT Responsibilities and Guidance, and in summary are:

- Ensure that Care Trust IT suppliers are capable of, and are enabling technology to fulfil this policy
- Ensuring that Care Trust IT suppliers are not violating the privacy and confidentiality of the Care Trust's communications or Internet Activity
- Enabling reporting systems to be in place between the Care Trust and the IT Suppliers
- Ensuring that IT supplier policy on Internet and Email usage does not create imbalance in the privileges that can be offered to Care Trust staff between different sites
- Ensuring that where appropriate, Care Trust IT suppliers are registered Data Controllers under the Data Protection Act 1998 (registered with the Information Commissioner).

4.7 Legal status of Emails and Internet Logs

The Care Trust and its staff should be aware that Emails and Internet logs and downloads constitute legal documents and records of the Care Trust. These qualities enable emails and internet usage logs to be accessible under the Freedom of Information Act 2000 and Data Protection Act 1998. Please see the section Appendix Nine - Freedom of Information and Data Protection Guidance for further explanation.

4.7.1 Ownership of Email

Staff should note that the Care Trust retains ownership of any email that is created or received by the Care Trust's email system(s). In this respect the Care Trust may open and review any stored email it has interest in, monitor or automatically scan traffic between staff and outside email addresses and may deny or delete email before or after it has been received by a staff member. Staff should be aware that they do retain the right to have their privacy respected, and that the Care Trust has a general duty of confidence towards its staff and the public. The Care Trust will in any event of monitoring or reviewing email follow the rules and spirit of the Data Protection Act 1998, Lawful Business Practice Regulations 2000, and Regulation of Investigatory Powers Act 2000. Guidance and requirements on monitoring activities is outlined in Appendix Eight – Monitoring Responsibilities and Guidance.

5 Appendix One – All Staff Responsibilities and Guidance

5.1.1 All Staff Responsibilities

All Staff are responsible for their own actions when using the Internet and Email Business Tools. Therefore all staff have the responsibilities to:

- Ensure their usage of the Internet and Email Business Tools are appropriate under the terms and guidance of this policy
- Have read, understood and agreed and to the terms and guidance of this policy.
- Prior to usage of these business tools, have read, understood, signed and dated the disclaimer associated with this policy

5.1.2 Identifying oneself

Any staff member using the Internet or Email business tools, or other business tools and/or services that interact with Internet or Email will be required, as appropriate, to identify themselves as Care Trust staff. In doing so staff will be honest, accurate and complete in their identity and function within the Care Trust. Staff should use professional looking signatures on their emails or any other material they post to the Internet. These signatures should:

- Include their last name, first initial or name, and business title
- Identify that they are an employee of the Care Trust
- Identify the unit, team or department of the Care Trust they work in
- Where appropriate, provide their contact information

An appropriate signature could look like:

Joe Blogs
Email Policy Writer
Camden and Islington Mental Health and Social Care Trust
Room 1, 1st Floor, Green Building,
Monarch Hospital
1 Neverland Road
London, NW1 0PE

Phone: 020 1234 5678
Fax: 020 1234 9876
Email: Joe.Blogs@candi.nhs.uk

5.1.3 Expression of Opinion

Any staff member using the Internet or Email business tools will be expected to represent the Care Trust unless they are using the tools for personal use. In doing so they will express Care Trust opinion, and only where requested supply their own opinion with the explicit identification that the opinion is their own. Where their personal opinion is offensive, defaming or derogatory they will politely decline comment so as to not associate the Care Trust or its business tools with their own opinion. Staff will also decline to provide offensive, defaming or derogatory personal opinions even when using the business tools for personal usage. Failure to do so may result in disciplinary actions as indicated in Appendix Five – Appropriate Usage Guidance and Mis-usage.

5.1.4 Authorisation to represent the Care Trust

Only those staff of officials so authorised to speak to the media, analysts or public on behalf of the Care Trust may speak or write in the name of the Care Trust. Whereas staff are expected to represent the ideals of the Care Trust when carrying out their responsibilities, they are not expected to make statements or step outside the scope of those responsibilities unless authorised to do so. The

Internet and Email business tools will provide a vast number of public venues in which staff may operate. Staff should therefore take care that their statements via these tools are representative of individuals working for the Care Trust and not, unless duly authorised, representations of the Care Trust as a whole. Onus falls therefore on the staff and their line management to ensure that correct representation is adhered too. The personal usage of these business tools does not negate this responsibility.
Individuals found to have violated this policy will be subject to discipline and/or dismissal under general misuse of the Care Trust's business tools, in addition to any discipline and/or dismissal that may result from other policies or legal obligations the Care Trust has in relation to the statements written and actions taken by the individual.

5.1.5 Spam and Junk Email

The Care Trust does not encourage the distribution of chain emails, spam or junk email. In particular the Care Trust strictly forbids mass emailing of such non-essential mail to staff within the Care Trust or to persons outside of the Care Trust. The personal usage of these business tools does not negate this expectation.

5.1.6 Global Emails

The Care Trust controls the emailing messages of the all members of staff ("global emailing"). Messages that staff or departments would like sent to all members of the Care Trust must be done through the Communication's Department. Staff members will be advised by the Communications Department as to what messages can be sent globally and when such emails will be sent.

5.1.7 Receiving the Personal Usage Privilege

The Care Trust recognises the personal use of its Internet and Email Business tools under Principle 3 of this policy (See Appendix Six – Business Tool's Policy Principles).
Staff will receive explicit permission for the use of the Internet and Email Business Tools by their line management. Staff and line management must have a recorded agreement as to the details and conditions of the Privilege granted. In particular written agreement should be made for unusual circumstances, for instance accessing otherwise denied sites for work purposes. Staff requesting individual instances of personal usage when they have not been given personal usage privileges require permission for the personal use, but it is not required in written form if this is impractical.
The personal usage privilege is defined in Appendix Six – Business Tool's Policy Principles.

5.1.8 When the Care Trust disagrees with the staff member on what constitutes appropriate usage under the Privilege

The Care Trust has the ultimate responsibility for the users of its Internet and Email systems, therefore has the ultimate say in what constitutes appropriate usage or the decision of the "reasonable person" under the Privilege. In practicality this means that line managers have both direct responsibility for their staff's usage of the Internet and Email and the definitive decision on what constitutes appropriate usage under the Privilege. Where staff and their line managers disagree over the definition of appropriate usage or the "reasonable person", either party may request a decision to be made, or guidance provided, at the next appropriate level of senior management.
Note that line management may not define what appropriate usage is, only

interpret what the Care Trust has provided in this policy.

5.1.9 Where use of the Privilege leads to negative consequences for Staff

Staff should take note that should their appropriate usage of the Privilege result in negative consequences to themselves, the Care Trust will take reasonable steps to defend them from those consequences. The Care Trust will only do so when staff have been granted the privilege of personal usage and have been found to be using that privilege appropriately.
For instance, staff using email appropriately, within the context of their Care Trust function, to contact service users will be defended if the services users complain that the emails were abusive or insulting.

5.1.10 Printing Personal Material

Printing for personal reasons will be at the discretion and expressed permission of the line management. It would be expected that whenever possible the printer be supplied with paper personally purchased by the staff wanting to print personal material.
Care Trust paper is not to be used for personal use and therefore cannot be bought from the Care Trust for this purpose.
Printing using the personal paper still costs the Care Trust money and resources; therefore line management should consider carefully the size and frequency of the requests. Inappropriate granting of printing requests will be deemed as misuse of the business tools by the line management and not the staff member. Unauthorised use of the printer or Care Trust paper for personal use will be deemed as misuse by the staff member and possibly by line management if the Care Trust finds them to be negligent or complacent to the situation.

5.1.11 Specific Privileges for the Internet

If the Privilege of personal usage is granted to a staff member, the Care Trust will endeavour to supply freedom for personal browsing of Internet. This will allow staff to browse non-work related sites within the kind acceptable to this policy (e.g. travel, humour, shopping, etc… but not derogatory, defaming, pornographic, etc…). This privilege will be granted for use during staff members' break and lunch periods unless otherwise arranged with line management.

5.1.12 Specific requirements for Email attachments

Attachments sent by Email cost the Care Trust, with greater costs being associated with the size of the attachment. Therefore large attachments or a number of attachments totalling to a large size (over 500 kilobytes) should be kept to a minimum when sending them for personal use. Staff would be wise to seek agreement from their line management before sending such attachments. Attachment also covers any pictures or icons that might be part of the email body itself.
Note that personal Email should only be done during break periods.

5.1.13 Specific requirements for Email disclaimers

Email disclaimers should not be altered by staff send emails. Where Care Trust Email is supplied using another organisation's system, staff will respect the use of that disclaimer. Staff should note that they are bound by the conditions of the Care Trust disclaimer as appropriate to its intention.

5.1.14 Reporting requirements

Care Trust staff have a requirement to assist in the maintaining of good practices and safeguards regarding the use of the Internet and Email Business

Tools. Staff should therefore actively work to help other staff understand and carry out good practice and report incidents/situations or concerns to their line management or appropriate helpdesk. Incidents or situations that would require reporting by a staff member include:

- Deliberate mis-usage of the business tools
- Security breaches or breaches of confidentiality using the business tools
- Abuse or harassment using the business tools
- Flaws or loopholes in technical security measures

6 Appendix Two – Management Responsibilities and Guidance

6.1.1 All Staff in a position of managing other staff

All line management staff are responsible for the actions of the staff that they have direct line management of. Therefore all line management staff have the responsibilities to:

- Have read, understood and agreed and to the terms and guidance of this policy
- Prior to providing their staff usage of these business tools, have read, understood, signed and dated their staff's declaration associated with this policy
- Appropriately provide the Personal Usage Privilege without prejudice or bias, and judge the granting of this Privilege on the basis of minimal risk to the Care Trust's time, resources and reputation and the competency of the staff on the Business Tools
- To proactively manage the risks to the Care Trust when providing the privilege of personal usage for the Internet and Email business tools to their staff
- Request any monitoring activity
- Ensure that disciplinary and dismissal procedures under this policy or in relation to this policy, are carried out fairly

6.1.2 Middle Management

Where staff have middle management responsibilities they will have the further responsibilities to:

- Ensure this policy is communicated, understood and represented within their team(s) and service(s)
- Monitor compliance to this policy for their team(s) and service(s)
- Ensure that there is adequate training on this policy in their team(s) and service(s)
- Authorise the granting of the Personal Usage Privilege for their team(s) and service(s)

6.1.3 Interpreting appropriate usage

Line management does not have discretion to define appropriate usage, only to interpret what the Care Trust has defined as appropriate usage. Further guidance on what the Care Trust believes to be appropriate usage can be found in Appendix Five - Appropriate Usage Guidance and Mis-usage.

6.1.4 Guidance on granting the privilege of personal usage

Granting personal usage of the Care Trust's Email and Business Tools should be considered in terms of the costs and risks to the Care Trust. Note that Internet and Email privileges should be considered separately. The definition of the personal usage privilege can be found in Appendix Six – Business Tool's Policy Principles. When granting the privilege consideration should be given to:

- Availability of computer resources
  - Do not tie up shared resources with non-essential usage
- Risk of distraction
  - If personal usage is granted exclusively for break periods, can the temptation for staff to be distracted outside their break periods be managed?

- Competency on business tools
    - For staff that have no competency what so ever on the Internet or Email no usage (even business usage) should be given until they have at least some training or demonstrate some experience. It may be appropriate to provide staff with minimal training and then some personal usage in order to encourage their development with the business tools.
- Previous offences
    - It may not be appropriate to grant personal usage to staff who have previously violated this policy. Assess the risk of re-offence and whether the situation of the previous offence would present itself again. Remember! – line managers are responsible for the actions of their staff and may be subject to discipline if they did not make reasonable efforts to ensure compliance with this policy.
- Workload
    - Only if granting personal usage outside staff break periods should line management consider workload issues. If workloads are high or there are priority tasks then privilege should not be granted outside regular break periods.
- New Staff
    - New staff should only be restricted in personal usage until such time as line managers are satisfied they are sufficiently competent in the business tool and this policy or relevant guidelines so as to not pose a risk to the Care Trust. Line Managers have the duty to ensure that new staff are trained quickly so that they are not unduly denied the personal usage privilege.

Things that should ***not*** be considered are:

- Performance of the employee
    - Staff are entitled to receive break periods regardless of their performance and what they chose to do during their break is not dictated by line management.
- Permanent Employment
    - All staff should have the same expectation of employment. Temporary, part time or volunteer staff should not be treated any differently than regular staff.
- Perks/Benefits/Disciplinary Action
    - The privilege of personal usage cannot be linked to any perk/benefit/disciplinary action regarding the member of staff, unless such thing applies specifically to the use of the Internet or Email Business Tools.
- Management Circumstances
    - The privilege cannot be denied because line management is not aware how to, or interested in, monitoring the staff member's activity. Line managers who are not comfortable with the technology should have this as part of their personal development plan. It would be acceptable to deny the privilege for a reasonably short period of time if line managers are

undergoing training to familiarise themselves with the business tools such that they can appropriately understand their usage and monitor staff.

Line managers and the staff member must have a written statement outlining the granted permissions. Line managers must document the justification for withholding or removing the privilege.

6.1.5 Recommended timing for personal usage privilege

Personal usage privilege should only be granted for regular break periods of the staff member. Staff that do not use their breaks for personal usage should not be given extra time to do so outside their regular break allotment unless there is specific and justifiable reason to do so.

It is recommended for line management to grant the personal usage privilege to be a blanket privilege during break periods and not require staff to receive permission with them for every instance of personal usage. It would not be appropriate for line managers to require staff to provide explanation for each personal usage or to have staff to keep personal usage records unless the privilege has not been granted.

6.1.6 Removing the Personal Usage Privilege

Line Managers may remove the personal usage privilege at any time for the following reasons:

- Documented abuse of the Internet or Email by the staff member, wherein the abuse is consistent with misuse outlined in this policy
- There is an ongoing investigation into possible misuse
- The cost (financial or otherwise) of providing the personal usage outweighs the Care Trust's interests in providing the privilege
- The risk of providing the personal usage outweighs the Care Trust's interests in providing the privilege

Line managers must provide staff written notification of the removal of the privilege and keep documentation as to the justification for this removal.

6.1.7 Printing Personal Material

Printing for personal reasons will be at the discretion and expressed permission of the line management. It would be expected that whenever possible the printer be supplied with paper personally purchased by the staff wanting to print personal material. Care Trust paper is not to be used for large personal use and therefore cannot be bought from the Care Trust for this purpose or authorised by line management.

Printing using the personal paper still costs the Care Trust money and resources; therefore line management should consider carefully the size and frequency of the requests.

Colour printing is an even greater expense to the Care Trust and as such all staff are encouraged not to print on colour printers for personal or business unless it has a black ink cartridge or the material is required in colour for business reasons. Where colour printing is requested for personal use, line management should carefully consider the size and frequency of those requests in regards to the cost or replacing colour cartridges for that printer.

Staff are encouraged to print double sided where it is appropriate and the printer can provide this.

Inappropriate granting of printing requests will be deemed as misuse of the business tools by the line management and not the staff member. Unauthorised use of the printer or Care Trust paper for personal use will be deemed as misuse

by the staff member and possibly by line management if the Care Trust finds them to be negligent or complacent to the situation.

6.1.8 Initiating Monitoring Procedures

Monitoring procedures can be requested from Executive members of the Care Trust when there is suspected abuse of the Internet or Email Business Tools. Further monitoring activity can be part of proactive measures to ensure compliance with this policy but would again require Executive permission. Further guidance on monitoring is found in Appendix Eight – Monitoring Responsibilities and Guidance.

6.1.9 Monitoring as part of proactive measures for policy compliance

Line managers are enabled and encouraged to use simple and minimal privacy invasive monitoring as part of their proactive measures to ensure compliance with this policy within their staffing responsibilities. These activities still require Executive consent however. Staff should always be asked for consent to these proactive measures, and if they refuse then this should be communicated to the Executive for permission to perform the activity. Note that refusal of consent does not deny the Care Trust the ability to monitor use of its business tools. Staff should always be given the opportunity to review and explain any material the investigating person deems inappropriate. Note that the Care Trust does not have the right to monitor email activity undertaken in any email account that is not linked to the Care Trust (e.g.: @hotmail.com or @yahoo.com accounts)

For Email monitoring the suggested activity:

- Occasionally sitting with the staff member and reviewing the titles of emails in their inbox and/or the email address they are sent to. Managers should be looking for emails have casual titles and the time they were sent. Email address that end in @yahoo.com, @hotmail.com or similar commercial email services should be checked occasionally for the times sent.
- If there are emails of interest due to the time or date of the email being sent, or the volume received or sent, the line manager may request an explanation of the staff member. Staff members will be expected to provide some information or their usage, and where they refuse, line management may “confiscate” a copy of the emails. These copies should be stored in whatever manner possible such that they are safe from opening prior to receiving permission from an executive or deleting/editing by either party until the matter is resolved. Suggested methods include:
    - Forwarding the emails as a batch to the next most senior manager, an executive or the Data Protection Officer (By selecting them all at once by holding the “ctrl” key down while clicking on the relevant emails to select them, then activating the forward function)
    - Creating a new password protected personal folder on the email system and saving transferring a copy of the email into there. This method is easiest if the staff member is available later to log into their email account.

For Internet monitoring the suggested activities:

- Scanning the hard drive or network storage using the “Search” function for key words relating to inappropriate material.

- Scanning the hard drive for file types such as pictures, executables or web pages.
- Reviewing a browser's history logs.

These activities should not be data collection activities. The only data that should be collected is where specific material has been deemed inappropriate and the line management has confiscated it for further action. Otherwise all data should be left on the machine it exists on, and no records created except to indicate how and why an activity took place, the outcome to the activity or the recording of a decision when made.
Where the investigation turns up something of interest, further monitoring exercises should be performed. Invasion of privacy however must be done in accordance with the guidelines of Appendix Eight – Monitoring Responsibilities and Guidance and new permission should be sought from Executive. Data may not be confiscated without prior permission from the staff member, or in case of staff member's refusal, the permission of an Executive. Personal use privilege may be legitimately denied during an investigation.

7 Appendix Three – Executive and Corporate Responsibilities

7.1.1 Responsibilities at Board Level

The Care Trust Board of Directors has overall responsibility for the appropriateness of this policy and its application. In particular it bears the responsibility to ensure any monitoring, interception, blocking and investigation proceedings are done fairly, and that the right of respecting individuals privacy is not forgotten.

7.1.2 CEO Responsibility

The CEO has reasonably the same responsibility as the Board, except in a more operational sense:

- It is likely that the CEO, or their designated representative, will be the only senior authority to be able to authorise any interception (as opposed to monitoring) activity. See Appendix Eight – Monitoring Responsibilities and Guidance for further information.
- Authorise the granting of the Personal Usage Privilege within the Care Trust

7.1.3 Senior Executive Responsibility

Senior Executives have responsibilities to:

- Ensure this policy is communicated, understood and represented within their directorate(s)
- Authorise any monitoring activity
- Monitor compliance to this policy for their directorate(s)
- Ensure that there is adequate training on this policy in their directorate(s)
- Ensure that disciplinary and dismissal procedures under this policy or in relation to this policy, are carried out fairly
- Authorise the granting of the Personal Usage Privilege within their Directorates
- If given the delegated authority to do so, authorise interception and investigation activities requiring further removal of privacy.

Senior Executive with responsibilities for IT may also have responsibilities under Appendix Four – IT Responsibilities and Guidance.

Note that executives are responsible for the decisions that staff may make beneath them in regards to the use of the Internet and Email policy. In practical terms the Care Trust will be enabled to take disciplinary action against executives who did not demonstrate sufficient fulfilment of their responsibility in ensuring their directorate(s) or corporate service(s) were sufficiently aware, trained or enabled regarding this policy.

7.1.4 Email Disclaimer

The Care Trust will install an email disclaimer for its outgoing emails. This disclaimer will be attached to all emails leaving the Care Trust's email systems. Where the Care Trust contacts IT services from another provider, it will ensure that there is an equivalent disclaimer on its outgoing email. The Care Trust Executive, or their appointed representative, will ensure that this disclaimer, or sufficiently similar disclaimer, will appear on any email written by Care Trust staff leaving any of the networks the Care Trust uses.

At minimum the Care Trust will use the email disclaimer below for emails sent outside the Care Trust email system. Note that this disclaimer has, with approval, been copied from the Information Commissioner's office, the body

responsible for the Data Protection and Freedom of Information Acts.

If you are not the intended recipient of this e-mail (and any attachment), please inform the sender by return e-mail and destroy all copies. Unauthorised access, use, disclosure, storage or copying is not permitted.

Communication by Internet e-mail is not secure as messages can be intercepted and read by someone else. Therefore we strongly advise you not to e-mail any information which if disclosed to unrelated third parties would be likely to cause you distress. If you have an enquiry of this nature please provide a postal address to allow us to communicate with you in a more secure way. If you want us to respond by e-mail you must realise that there can be no guarantee of privacy.

Any e-mail including its content may be monitored and used by the Camden and Islington Mental Health and Social Care Trust for reasons of security and for monitoring internal compliance with the office policy on staff use. This includes the content of e-mails. E-mail monitoring / blocking software may also be used. Please be aware that you have a responsibility to ensure that any e-mail you write or forward is within the bounds of the law.

Camden and Islington Mental Health and Social Care Trust cannot guarantee that this message or any attachment is virus free or has not been intercepted and amended and you should perform your own virus checks.

---

http://www.candi.nhs.uk

Camden and Islington Mental Health and Social Care Trust, St. Pancras Hospital, 4 St. Pancras Way, Camden, London, NW1 0PE

Tel: 020 7530 3500

7.1.5 Technical vs. Managerial policy enforcement

The Care Trust recognises the need and benefits of using technology to support this policy. Such technology as Internet filters, Email and virus scanners and automated logging systems provide the Care Trust the tools to ensure that it is gaining maximum potential from its Internet and Email business tools. However the Care Trust commits itself to being proactive in the management of these tools and not to rely solely on technology to enforce this policy. It does so because it understands that technology is fallible, avoidable and unable to monitor the vast number of circumstances in which the Internet and Email services can be used.

7.1.6 Declaration description

The Care Trust will require staff members to sign a declaration of their understanding and willingness to abide by this policy before being given access to the Internet and Email Business tools.
This Declaration will be recognised as a contract between the staff member and the Care Trust. Staff members on networks supplied by other organisations will be required to sign the Care Trust's declaration as well as any declaration the other organisation may request relating to the network.

7.1.7 Care Trust Declaration for usage of the Internet and

The Care Trust will use the following declaration. It will be the responsibility of the Care Trust Executive, or their appointed representative, to ensure that this declaration is provided as a condition of being given any usage of the

Email

Internet or Email Policy.

“

I have received, read and understood the Care Trust’s Internet and Email policy and agree to abide by the terms and guidance of this policy.
I understand that:

- I am not to share my Email or Internet account passwords unless there is a legitimate business need, authorised by my manager, to do so.
- Any confidential material received or created using the Internet or Email Business Tools is to be respected appropriately as confidential.
- The Care Trust retains sole ownership or custodianship of any data or information created on, or transferred onto, its networks by the use of the Internet and Email business tools.
- The Care Trust will have automated procedures and technologies that collect personal information about my usage of the Internet and Email Business Tools and that it may access this information under reasonable circumstances as dictated under statute and law.

I accept that:

- The Care Trust may, under reasonable circumstances, engage in monitoring, interception, blocking and investigatory procedures that may require access to material that is confidential and personal information that I am responsible for.
- I cannot expect complete privacy or confidentiality of material I receive or make.
- Violation of this policy may lead to disciplinary or dismissal procedures, as well as any other such procedures, including criminal proceedings, that may result from the Care Trust’s other obligations under statute, law and/or policy.

“

This section of the declaration will be accompanied by:

- Spelt Name of the Staff Member signing
- Signature of the Staff Member
- Date of the Signature
- Title of the Staff Member

The declaration will also have a second section relevant to the line management of the staff member applying for the business tools:

“

I, as the direct manager of said staff member above, understand that:

- It will be my responsibility to ensure that the said staff member will follow the terms and guidance of the Care Trust’s Internet and Email policy.
- In my management of said staff member, I have read and understood the Internet and Email policy, and where appropriate will apply the Privilege of personal use under the guidance given by the Care Trust.
- Should I not undertake proactive steps in line with this policy, statue and law, to ensure that the said staff member does not violate this policy, or the said staff member violates this policy due to my

negligence, complacency or unwillingness to enforce this policy, I may be subject to disciplinary or dismissal procedures under this policy as well as any other such procedures, including criminal proceedings, that may result from the Care Trust's other obligations under statute, law or policy.

"

This section of the declaration will be accompanied by:

- Spelt Name of the Manager signing
- Signature of the Manager
- Date of the Signature
- Title of the Manager

7.1.8 Training opportunity

The Care Trust will commit itself to providing sufficient training opportunities to those staff that wish to use the Internet or Email business tools. In particular it will consider the ability of those in line management responsibility to receive sufficient training as to be able to proactively monitor staff usage of the Internet and Email Business Tools.

8 Appendix Four – IT Responsibilities and Guidance

8.1.1 Senior Executive Responsible for IT

The Senior Executive(s) Responsible for IT will be required to ensure that the Care Trust's IT suppliers are:

- Capable of, and are enabling technology to fulfil this policy
- Capable of, and are providing sufficient service to fulfil this policy
- Are not violating the privacy and confidentiality of the Care Trust's communications or Internet Activity.
- Are undertaking monitoring activities in accordance to, and by direction from, the Care Trust.
- Enable reporting systems required from this policy to be in place between the Care Trust and the IT Suppliers

8.1.2 IT Suppliers as registered Data Controllers

This policy expects that the IT suppliers who provide the Care Trust's Internet and Email Business Tools will have registered with the Information Commissioner as Data Controllers, as required under the Data Protection Act 1998. More information can be found at the Information Commissioner's website: http://www.informationcommissioner.gov.uk/

8.1.3 Where the Care Trust's Internet and Email policy is different to the Supplier's

The Care Trust will expect its staff members, or members of staff seconded to the Care Trust to abide by the Care Trust's policies when using the Internet and Email business tools. Except wherein the Supplier's policy requires greater security or has more stringent protocols specific to the content of material allowed on its network, the Care Trust's policy will take precedence.

8.1.4 Use of Email Disclaimer

The Care Trust will ensure that the disclaimer agreed within this policy will be represented, or have similar representation, on the emails sent outside of the suppliers' local networks. The email disclaimer can be found in Appendix Three – Executive and Corporate Responsibilities.

8.1.5 Use of Email and Internet declaration

The Care Trust will ensure that its suppliers do not provide access to the Email or Internet business tools for those staff who have not signed, and had their managers sign, their declaration. The declaration can be found in Appendix Three – Executive and Corporate Responsibilities.

8.1.6 Maintaining registers

The Senior Executive(s) Responsible for IT will be required to keep a register of all the Care Trust staff's email addresses. This register must be kept up to date and at minimum identify the name of the staff member responsible for the account, their line manager, and the email address.
Additionally a register of active Internet accounts must be kept, at minimum capturing the name of the staff member responsible for the account, their line manager, the email address and the level of access they have on the network.
The executive(s) must also ensure that Care Trust's IT supplier are informed of staff departures and that the suppliers remove the various accounts and permissions from the system of the previous staff.

9 Appendix Five – Appropriate Usage Guidance and Mis-usage

9.1 Framework for Appropriate Usage

This policy is based on the Care Trust's understanding that its staff are responsible and dependable employees. In doing so it has given staff the ability to monitor their own activity on the Internet and Email to ensure that they are using the business tools appropriately. However human nature being what it is, the Care Trust ensures appropriate usage through mild, occasional and controlled "checks" of previous activity. Only where mis-usage is suspected or discovered will heavy invasions of privacy occur.
In giving staff this responsibility for their own usage the Care Trust has provided guidance in the form of questions, to be used with the "reasonable person principle" as well as a list of definite mis-usage activities.

9.1.1 Definition of a Reasonable Person

This policy depends on the "reasonable person principle". For the purpose of this policy a reasonable person is similar to the "reasonable man" in principles of UK law. The reasonable person is a summation, or average of societal opinions and knowledge. This is different than the "ordinary man" of UK law, who is assumed to be somewhere between the extremes of unusually suspicious and unusually naive.
Because of the impossibly objective nature of the Reasonable Person, it is expected that appropriate use of the Internet and Email will generate some discussion between staff and their line management.

9.1.2 Responsibilities of the Reasonable Person

When staff or their line managers make decisions on behalf of, or in assumption of the Reasonable Person principle, they will be making decisions for which they are personally responsible. This responsibility, as set by this policy, will be linked to professional competency. If at any time the decision is an uncomfortable one for the decision maker, they are expected to seek guidance or a decision from their line management.
It is important to note that line management is responsible for the decisions and actions of their staff, and could face discipline or dismissal if they fail to ensure appropriate use of the Internet and Email by their staff.

9.1.3 When the Care Trust disagrees with the staff member on what constitutes appropriate usage

The Care Trust has the ultimate responsibility for the users of its Internet and Email systems, therefore has the ultimate say in what constitutes appropriate usage or the decision of the "reasonable person". In practicality this means that line managers have both direct responsibility for their staff's usage of the Internet and Email and the definitive decision on what constitutes appropriate usage. Where staff and their line managers disagree over the definition of appropriate usage or the "reasonable person", either party may request a decision to be made, or guidance provided, at the next appropriate level of senior management.
Line management does not have discretion to define appropriate usage, only to interpret what the Care Trust has defined as appropriate usage.

9.2 Appropriate Usage Questions where no personal usage has been given

The guidance questions below are to be used during normal business use of the Internet or Email Business Tools.

9.2.1 Question 1

Any activity on the internet may be inappropriate if it is not used for a business purposes. Therefore the first question would be:

> "Am I using the Internet or writing this email in pursuance of my duties as a Care Trust employee?"

Where the answer is No, staff should discontinue or not begin using the Internet or Email systems for that particular purpose. Where the answer is Yes, the staff should ask the second question (see section Question 2).
This question is to assess whether the usage of the Internet or email is for the business of the Care Trust. This question is all encompassing, but should be fairly easy to assess. Simple guidance examples would be:

- Booking tickets
  If the tickets were to take a business trip, then this would be appropriate use of the Internet. If the tickets were for a concert or a trip during vacation it would be inappropriate.
- Write an email to a friend or chatting online with friends about the weekend
  This would be inappropriate, as communication not involving Care Trust business is not helpful to the Care Trust.
- Looking up a website explaining a disease process
  If the information is being sought to improve the care of a Care Trust's client then this is appropriate, however if it is to improve the care of a family member not under the care of the Care Trust, it is inappropriate.

9.2.2 Question 2

When the first question enables the use of the Internet and Email for business purposes, the second asks if it is the appropriate and best usage of these business tools. Therefore staff should ask the following using the "reasonable person principle":

> "If a reasonable member of the public, knowledgeable about my duties and responsibilities, conscious of their public tax monies being spent and having expectations of a professional NHS, were to be watching over my shoulder would they object or question my accessing the Internet or writing of this email?"

Where the answer to this question is Yes, staff should consider the method by which they are trying to achieve their goal and change it so that they are more in line with what a reasonable member of the public might expect. If the answer is No, then the staff will be justified in using the Internet or Email systems.
This question addresses the method by which staff use the Internet or Email and the suitability of the use in the larger context of their responsibilities. In particular this question is to help prioritise the usage of the Internet and the professionalism by which an email is written. Again this is an all-encompassing concept, but should be fairly easy to assess. Simple guidance considerations are below:

- Multiple duties

  If your duties require access to the Internet or answering/writing an email to complete a priority task then the usage is appropriate. If there are other more pressing responsibilities than the one requiring use of the internet or answering/writing email then the use would be inappropriate.
- Professionalism

  If the specific Internet page I am looking at has questionable content, or is not particularly well related to the task being performed then it is probably inappropriate. For instance, it is not appropriate to review pornography to study anatomy.

9.2.3 Question 3

Where question one and two address issues of appropriate usage, question three specifically relates to how a staff member uses Internet and Email. Therefore a member of staff should ask themselves, using the "reasonable person principle":

> "If a reasonable member of the public were to review my writings or actions on the Internet or Email, out of the context of which they were written or performed, would they be able to reasonably assume that I was acting or writing in a professional way and am a member of a respectable and professional organisation?"

Staff members are expected to use the Internet and Email in a professional way, so that they and the Care Trust retain a professional respectability. Where appropriate the Care Trust will monitor the activities of staff to ensure that a high level of professionalism is maintained. This question does not preclude staff from using unprofessional writing or acting in unprofessional ways where the circumstance necessitates it. For instance, if staff need to quote words used by another that are derogatory, disgusting or defaming for the purpose of the discussion (perhaps to quote a service user's particular behaviour), then their actions would be acceptable. This does not give free licence however, as it would obviously be in the staff member's and Care Trust's best interest if such writings or actions were tempered or described politely wherever possible. Other considerations would be:

- Professionalism

  How professional will the email that I am writing or responding to appear to the recipient or to a reasonable member of the public? If I am allowing email to come to myself from colleagues, or creating such emails, that if taken out of the context would not look like a professional conversation to a reasonable member of the public it is probably inappropriate.
- Using Alternatives

  If I appear to be acting or writing in an unprofessional way, despite having good reason to, but I know of another reasonable way to accomplish the same goals without looking unprofessional then it is probably more appropriate to use the latter method.

9.3 Appropriate Usage Questions where personal usage has been given

Below are the guidance questions to be used when the privilege of personal use has been granted for the Internet and Email Business Tools. Note that the questions below replace the three above during personal usage. These questions cannot be used to circumvent mis-usage or other specified mis-usage given in the policy.

9.3.1 Changing the Appropriate Usage Questions

When enacting the privilege the Care Trust negates or changes the questions staff may ask of themselves when seeking guidance as to appropriate usage (These questions can be found under the Sections: Question 1, Question 2 and Question 3). Staff are to substitute the questions below for guidance when they are engaging in the privilege. Note that the questions below do not replace the original appropriate usage questions during the normal business usage of the Internet and Email Business tools.

9.3.2 Appropriate Usage under the Privilege Question 1

When engaging in the Privilege of person use, staff should ask themselves the following question using the "Reasonable Person Principle" (as defined above):

> "If my activities using the Care Trust's Internet and/or Email were being observed by a reasonable member of the public, who is conscious of and respects human nature and expects reasonable self-discipline, professionalism of NHS and Care Trust staff and value of tax monies, would they have cause to question or disagree with my activities or writings?"

This question attempts to address the appropriateness of the personal usage. If the answer is No, then staff are not likely to be using the privilege appropriately. Although staff are able to use the business tools for personal use, the tools themselves are associated with the Care Trust, and therefore any usage of them reflects back upon the Care Trust and its staff. Examples to consider:

- Things you may find appropriate, but the majority may not expect the NHS to support. For instance, reviewing crude yet funny jokes is not likely to be appropriate.
- The "Child Test"
  Generally if the material is such that it would be not appropriate for a child to view, despite the ability of a child to understand, it will be inappropriate.

9.3.3 Appropriate Usage under the Privilege Question 2

Where the first question is Yes, staff should ask themselves the following second question using the "Reasonable Person Principle" (as defined above):

> "If my activities, both in light of content and time spent, on the Care Trust's Internet or Email were to be reviewed outside of the context of the situation, but within context of this privilege, would the Care Trust's resources, reputation and professionalism, business and interest and/or staff (including myself) be at risk?"

This question is similar to the first but approaches the concept from a different angle. If the answer is Yes, then staff are not likely to be using the Privilege appropriately. If the answer is No, then staff are likely all right in their activities.

Things for staff's consideration are:

- Length of Time

  If you are using the Privilege, make sure you are using it within the periods or constraints it has been supplied to you under

- Outside perceptions

  Would someone be able to reasonably make an issue over my activities, for example consider if a report had a log of all the websites I accessed, would there reasonably be something to report in the interest of the public?

9.3.4 When the Care Trust disagrees with the staff member on what constitutes appropriate usage under the Privilege

The Care Trust has the ultimate responsibility for the users of its Internet and Email systems, therefore has the ultimate say in what constitutes appropriate usage or the decision of the "reasonable person" under the Privilege. Where disagreements occur, the same protocol given above for a disagreement can be used.

9.4 What constitutes Misuse?

This section outlines what the Care Trust will consider as specific misuse and the actions the Care Trust will take if it discovers misuse. These listed Misuse criteria are in concert with the 4 Principles (found in Appendix Six – Business Tool's Policy Principles) and 5 Guidance Questions listed above so that violations under these specific Misuses will most likely also be viewed as a violation the 4 Principles and 5 Guidance Questions.

9.4.1 Repercussions of Misuse

The Care Trust will not tolerate misuse of its Internet and Email. The Care Trust considers the usage of its Internet and Email business tools to be linked with professional competency. It may, depending on the severity of the situation or repetition of similar situations, apply discipline and dismissal procedures against staff who have been found to be misusing the Internet or Email under this policy and any other policy or obligation it may have in regards to the actions and materials held by the individuals involved. Line Management should be aware that because they are directly responsible for the actions of their staff that they may face discipline or dismissal should the Care Trust find that inappropriate usage of the Internet and Email business tools have occurred with their consent or connivance, or by their negligence.

9.4.2 General Disclaimer about Misuse

The topics listed below will in almost all cases fall into the category of misuse of the Care Trust's business tools. However in the particular cases of Internet material it may be appropriate for legitimate business reasons for staff to have access to material otherwise deemed as inappropriate. If this is the case, their line management will need to supply written permission to the Care Trust's IT department in order to allow the technical filters to be removed and recorded permissions to be established. For situations not involving Internet content, staff members must obtain written permission from their line management.

9.4.3 Sexually Explicit Material

The Care Trust strictly prohibits the downloading, transfer, processing, capture and storage of sexually explicit images, documents, media or executables using any of its systems. Individuals found to have violated this policy will be subject to discipline and/or dismissal under general misuse of the Care Trust's business tools, in addition to any discipline and/or dismissal that may result from other policies or legal obligations the Care Trust has in relation to the sexual explicit

material or the actions taken by the individual with such material.

9.4.4 Offensive, Derogatory and Defaming Material

The Care Trust strictly prohibits the downloading, transfer, processing, capture and storage of offensive, derogatory and defaming images, documents, media or executables using any of its systems without clear and legitimate business need. In particular the Care Trust prohibits the use of its Internet and Email to create or disseminate such material without clear and legitimate business need. Individuals found to have violated this policy will be subject to discipline and/or dismissal under general misuse of the Care Trust's business tools, in addition to any discipline and/or dismissal that may result from other policies or legal obligations the Care Trust has in relation to the offensive, derogatory and defaming material or the actions taken by the individual with such material.

9.4.5 Staff responsibilities when encountering Sexually Explicit, Offensive, Derogatory and/or Defaming Material

The Care Trust will deny access to inappropriate or sexually explicit Internet websites using automated processes. When such a site is accidentally discovered by a user they should note the site's addressing and method they arrived there, then immediately disengage from the site. Users should then report the sites address and the method arrived there to a Care Trust IT helpdesk as soon as practical.
Note that sites that are not blocked by the Care Trust's processes are not by this characteristic deemed acceptable sites. Sites that are obviously or borderline inappropriate sites that are accessible to staff should be reported to the IT helpdesk. If an individual is found to have repeatedly visited an inappropriate but accessible sites without reporting, and subsequently the Care Trust discovers and deems it inappropriate, the individual may be subject to discipline and/or dismissal under general misuse of the Care Trust's business tools.

9.4.6 Copyrighted or Trademarked Material

The Care Trust strictly prohibits the downloading, transfer, processing, capture storage and usage of copyrighted or trademarked images, documents, media or executables using any of its systems without legitimate business reasons and the consent of the copyright or trademark holder. The Care Trust also strictly prohibits the uploading to the public Internet of any copyrighted or trademarked images, documents, media or executables under licence by the Care Trust or any other entity.
Where it is necessary for such transfers to occur, such undertaking should be done with written authority of the staff's line management and the relevant copyright or trademark holding department and undertaken either by a Care Trust IT helpdesk or with the written authority of a Care Trust IT helpdesk. Virus checking software should be used to scan any such material.
Individuals found to have violated this policy will be subject to discipline and/or dismissal under general misuse of the Care Trust's business tools, in addition to any discipline and/or dismissal that may result from other policies or legal obligations the Care Trust has in relation to the copyrighted or trademarked material or the actions taken by the individual with such material.

9.4.7 Unlawful Activities

The Care Trust strictly prohibits the usage of its Internet and Email business tools for use in unlawful or criminal activities under law or regulation in the UK or any other nation in which the activity is affecting. Such activities may include, but are not limited too:

- Fraud and/or misrepresentation of identity
- Mischief or Harassment
- Intentionally spreading malicious software (e.g.: viruses)
- Intentional disruption of networked services (Care Trust or other)
- Dissemination of defaming, slanderous or hate material
- Communication or coordination of unlawful or criminal activities
- Illegal or unlawful monitoring of persons or organisations
- Illegal or unlawful collection of information

Individuals found to have violated this policy will be subject to discipline and/or dismissal under general misuse of the Care Trust's business tools, in addition to any discipline and/or dismissal that may result from other policies or legal obligations the Care Trust has in relation to the actions taken by the individual.

9.4.8 Political or Commercial Material

The Care Trust strictly forbids the usage of its Internet and Email business tools to propagate political or commercial material or messages that are not held and explicitly endorsed by the Care Trust. Note that legitimate Trade Union activity is unlikely to fall into this category. Individuals found to have violated this policy will be subject to discipline and/or dismissal under general misuse of the Care Trust's business tools, in addition to any discipline and/or dismissal that may result from other policies or legal obligations the Care Trust has in relation to the material publicised or actions taken by the individual.

9.4.9 Circumvention of Established Network Protocols and Architecture

The Care Trust strictly prohibits the circumvention of its established network protocols and architecture without justified business reasons. This includes, but is not limited to:

- Use of alternative, or disablement of, proxy servers
- Circumvention of established routing
- Use of alternative mail servers
- Disablement of encryption or secure network protocols
- Disablement or circumvention of virus or heuristic checking software
- Establishment of alternative network portals
- Intentional bridging of the Care Trust's network to another
- Modification of Email disclaimers

In the case where a staff member has a justified business reason(s) to circumvent the established network protocols and/or architecture they would be well advised to receive signed permission from the Care Trust's IT department/supplier and their line management.

9.4.10 Gaming

The costs of providing Internet and Email business tools is linked directly with usage. The Care Trust therefore strictly prohibits the use of networked games. Individuals found to have violated this policy will be subject to discipline and/or dismissal under general misuse of the Care Trust's business tools.

10 Appendix Six – Business Tool's Policy Principles

10.1.1 Principle 1

The Care Trust will not tolerate use of its IT, network and e-mail systems that is not directly related to Care Trust interest or business. Any activity that is not consistent with the business or interest of the Care Trust will be deemed as a misuse of the Care Trust's business tools and exposes the individual performing these activities to discipline and/or dismissal under general misuse of Care Trust resources, in addition to any discipline and/or dismissal that may result from other policies or obligations the Care Trust has in relation to the activity of the individual using the business tools.

10.1.2 Principle 2

The Care Trust provides Internet and e-mail services to its staff as business tools. These tools are the property of the Care Trust and any material produced or received via these tools are either under the ownership or custodianship of the Care Trust. Individuals may not claim personal ownership or custodianship of any material transferred to or created on the network or e-mail system regardless of subject matter, and hence should be aware that there is no absolute guarantee of privacy or confidentiality while such material exists on the Care Trust's network. The Care Trust will however follow the rules and spirit of the Data Protect Act 1998, Lawful Business Practice Regulations 2000, and Regulation of Investigatory Powers Act 2000 in protection of individuals' rights to expect privacy of their personal information. In accordance with these regulations the Care Trust will monitor the activity of its business tools, but will only monitor individuals' use of these tools in the limited circumstances where it feels is necessary.

10.1.3 Principle 3

The Care Trust does not provide Internet access and email as a replacement for staff independently acquiring and paying for such services themselves. The Care Trust does however recognise that such services are personal conveniences for staff and that in given cases limited and reasonable use aids the wellbeing and satisfaction of its staff. The Care Trust may therefore extend a privilege to staff to use the Care Trust's business tools for personal use under appropriate and limited circumstances. This privilege would require staff to respect the boundaries in which the privilege is given and would be provided on the continual respect of those boundaries and business circumstances of the Care Trust. This privilege would not enable staff to use the Internet access and email in ways incompatible with the ideals or business of the Care Trust and to do so could result in discipline and dismissal for the offending staff. This privilege and the assessment for granting it would be independent of any other privileges or disciplinary procedures. This privilege should not be an expectation of employment or an expectation of being granted when given the business tools themselves. When enacted, Principle 3 overrides Principle 1 and allows for personal use of the Internet and/or email services without repercussions, so long as this usage does not compromise the Care Trust's business, reputation or professionalism. Further explanation of this privilege is provided under the definition of the personal usage privilege below.

10.1.4 Principle 4

The Care Trust will provide policy and guidance to its staff so that they are made aware of what constitutes acceptable usage of these business tools, the penalties for misuse, the limitations of any privileges granted and the reasons and ways in which monitoring may take place.

10.1.5 Definition of personal use privilege as granted by Principle 3

The Definition of this privilege is as follows:
The Care Trust will grant personal usage of its Internet and Email business tools to a staff member when the limited and respectful use of the business tools will not significantly affect the performance of the said staff's business functions and the staff member does not endanger or disadvantage the Care Trust through this personal usage. This usage will be at the discretion of line management, and is not an automatic privilege granted with employment, good performance or as any, or linked to any, type of perk/benefit of being employed by the Care Trust. As the privilege is not linked to a perk/benefit of working for the Care Trust, payments or benefits in lieu of this privilege are not possible, and the privilege cannot be linked to any accolades, performance or disciplinary measures that do not involve the usage of these specific business tools. The privilege will only be enabled in situations where detriment to the Care Trust is minimal and staff are judged to have sufficient competency in using the business tools, and may be suspended by line management or the Care Trust due to workload or business reasons, misuse or other legitimate reasons. The personal usage will be limited in time and/or other factors such as, but not limited to; storage space, content of material, risk to Care Trust property and resources and public perception of the Care Trust.
The granting of the privilege does not remove or change the policy in any other way except where stated. The Privilege may be granted for both Email and Internet or separately, at the discretion of line management or the Care Trust.

11 Appendix Seven – Good Practice Guidance

11.1 Internet Specific Points

This section deals specifically with policy statements related to the Internet business tool.

11.1.1 Chat rooms and Newsgroups

Where staff are to participate in a chat room, newsgroup posting board, etc… when using the Care Trust's internet they should inform their line management. In doing so they will provide any relevant information needed to find and identify their usage of such sites. Line Management may deem the site inappropriate to be accessed using the Care Trust tools if the site's materials or discussions are not appropriate to be linked to the Care Trust.

11.1.2 Providing details to commercial sites

When engaging in personal consumer activity it would be inappropriate to provide your Care Trust contact details to any commercial sites. In doing so you may at the very least inadvertently enables the Care Trust to receive unsolicited advertisement.

11.2 Email Specific Points

This section deals specifically with policy statements related to the Email business tool.

11.2.1 Email Account Responsibilities

Care Trust staff will be given responsibility for their own personal business email account. Because staff are not to share their account passwords with other members of staff and where email accounts are shared a disclaimer is expected informing people that the account is shared, it will be assumed that any emails originating from their account will be from them. This means that should a member of staff deliberately or inadvertently provide their email account for usage by another person that the member of staff will still be liable for any email that comes from their account. The only exception is when line management has provided permission for a second staff member to have access to the account for continuation of business reasons, in which case the line manager and the second staff member are responsible for those emails written on the account in the staff member's absence.
It is therefore highly recommended that staff log off, lock-out or otherwise protect their computers, passwords and account details from discovery or use by any others.

11.2.2 Use of confidentiality markers

Where staff are involved with confidential discussions between themselves or members of the public they would be well advised to mark the email as confidential or private. This may be done, if supported by the email system, through the use of "flags". The use of flags is not particularly recommended due to the possibility of incompatible email systems. The recommended method is to indicate that the email is private/confidential in its title or subject line.

11.2.3 When postage is more appropriate

The Care Trust encourages staff and the public to submit sensitive confidential and private information by postage. For staff the Care Trust recommends that particularly sensitive private/confidential material should be sent to the via the post, particularly if going to the following departments/services:

- Occupational Health
- Trade Unions

- Legal Advisory or Solicitors
- Complaints

11.2.4 Staff Receiving Personal Emails

The Care Trust realises that staff members may receive emails of a personal nature, and that they may not have reasonable control over this. However the Care Trust will expect that staff limit supplying their business email to members of the public or businesses outside of Care Trust business requirements, particularly when no personal usage has been granted. Where the Care Trust finds that excessive personal emails are being sent it may take steps to block such emails from being received, and where activities are harassing to the staff member, take appropriate action against the sender.
The Care Trust does recognise that email may be an appropriate and reasonable method for emergency personal contact. This, and only in this limited case will the Care Trust allow reasonable and limited personal use of the Care Trust's business tools when no personal usage privileges has been granted. Staff members in such a situation should inform their line management as soon as possible and may be required to provide proof of such emergency, possibly including line management access to the communications in question. Failure to inform line management may result in Disciplinary measures being taken.

11.2.5 Netiquette

Emails and Internet communications have their own particular communication style. Although not as necessary purely for professional writings, knowing the etiquette of this communication is useful so as to not inadvertently offend someone. Staff may find etiquette guidance in a separate document titled "Email Etiquette Guidance (Netiquette)".

12 Appendix Eight – Monitoring Responsibilities and Guidance

12.1 Monitoring, Interception, Blocking and Investigations

This section outlines how and when the Care Trust may enact monitoring, interception and blocking procedures on the Internet and Email business tools.

12.1.1 Risk Management

The Care Trust recognises that in providing the business tools of Internet and Email it has potentially enabled staff to be more productive and provide better care to their patients and the public they serve. The Care Trust also recognises that in providing these business tools it has created a potential for misuse and distraction. The Care Trust therefore wishes to manage this risk to protect itself, staff members it is responsible for, and the public it serves. In doing so it will have occasion/situation wherein it will have the necessity to monitor the activity of individual members of staff, review confidential information about staff, patients and members of the public, block or intercept communications and/or block staff from accessing specific Internet sites. When engaging in these activities the Care Trust will take utmost care to preserve the dignity, privacy and respect for its staff, patients and public.

12.1.2 Informing of Monitor or Interception

The Care Trust will inform its staff when it is intercepting or monitoring Internet or Email activity in connection with themselves and the justification for such activity. Covert monitoring or interception will only take place when the Care Trust suspects serious unlawful or criminal activity, gross misconduct or malpractice is taking place, or at the request of organisations that have the ability to authorise covert monitoring.
Staff should be aware that the Care Trust does not require consent from staff in order to begin monitoring. If the Care Trust does approach staff for consent to monitor or intercept, staff should be aware that even if they refuse they might not be able to prevent the monitoring or interception from taking place. When consent is required the Care Trust will ensure:

- It is Explicit (i.e. provisional on the monitoree's signature)
- Freely given (i.e. such that there is real choice and no significant detriment to refusing)

12.1.3 Blocking in general

The Care Trust will, where technologically feasible and as a pre-emptive measure to prevent misuse and distraction, block staff access to specific Internet sites and Email addresses that it knows to have inappropriate or potentially harmful material. The Care Trust will update this list as it sees necessary.
Where staff have legitimate business reasons for accessing sites the Care Trust has blocked, they should present written permission from their line management to the Care Trust's IT helpdesk asking for the block to be removed. This removal will only be enacted for a limited time, as agreed with the line management, and re-assessment of the access will be the responsibility of the staff member and their line management.

12.1.4 Investigations

Investigations are the retrospective examination of stored information relating to a specific individual. The information, in particular emails, that an investigation would examine must have been reviewed by the staff member

first in order for it not to qualify as interception. Investigations do not require consent from staff members, however the same safeguards of confidentiality and privacy will apply as it does with monitoring and interception.

12.1.5 Information Collected as part of a Monitoring or Interception Exercise

When collecting information by a monitoring or interception exercise the Care Trust will collect it under and treat it as personal information under the Data Protection Act 1998. This means when collecting information it will:

- Have defensible reasons to collect each specific type of information
- Have defined and specific usage for that information and will not use that information for purposes outside that usage
- Have a define time period it will hold that information (usually no more than 6 months after the purpose of the information is fulfilled)

The Care Trust will not however ignore information or prevent itself from taking action where it discovers information that an employer or Trust could not reasonably ignore.

In treating the information collected as personal information under the Data Protection Act, this information will:

- Be accessible to the staff member it relates to under the Data Protection Act, including the ability to request changes, corrections and deletions of errors or misrepresentations.
- Be treated as confidential, and therefore will be accessed by the minimum number of people.
- Will not in itself form part of a permanent record

If this information is to be used in a formal Discipline or Dismissal process, the staff member the information relates to will be provided with opportunity to view the information and comment, present arguments and/or corrections against that information.

Information collected, particularly Care Trust wide monitoring information, may be accessible to the public under the Freedom of Information Act 2000 and Data Protection Act 1998. Please see the section Appendix Nine – Freedom of Information and Data Protection Guidance for more information.

12.1.6 Situations where Monitoring may take place

The Care Trust will limit the situations in which it will perform Monitoring at a level of scrutiny to be able to identify individuals. This does not include automated monitoring or interception, as classified by actions taken by a machine or software that does not involve information being read or reviewed by a human being.

The Care Trust will not perform invasive monitoring on staff on a regular and continual basis without sufficient justification to do so. The Care Trust will not monitor staff:

- As part of a disciplinary action
- To intimidate or exert pressures not related to the correct usage of the business tools

The Care Trust may monitor staff only:

- For the performance and protection of Care Trust business and obligations, which may include:
  - As part of training, with the staff's awareness
  - As part of competency assessment, with staff's awareness
  - As part of a complaint or investigative procedure
  - For random sampling of business tool usage, with staff's awareness

- Prevention or detection of unlawful or illegal activities
- On the appropriate request of the staff member to be monitored
- As part of the proactive measures to ensure compliance with Care Trust policy

12.1.7 Situations where Interception may take place

The Care Trust will only engage in interception in the limited circumstances where serious unlawful or criminal activity is suspected/known or with the explicit consent of the individual staff member. This does not include automated monitoring or interception, as classified by actions taken by a machine or software that does not involve information being read or reviewed by a human being.
This also does not include interception done as part of the requirement for continuity of Care Trust business while a member of staff is absence and cannot collect their emails.

12.1.8 Situations where Investigations may take Place

Investigations may take place for any reason that requires the Care Trust to check back upon activity of its staff. This may include, but is not limited too:

- Complaints
- Assessment of Malpractice, Misconduct or Unlawful/Criminal activity
- Freedom of Information or Data Protection Requests
- Auditing
- Record Keeping
- Local & Serious Incidents

Staff should be aware that the Care Trust does not require consent to open emails already received and read by the recipient, or to trace previous usage of the Internet. The Care Trust continues to be obligated to Data Protection and similar requirements and will treat information gained from these exercises as appropriate.
Information gathered as part of an Investigation will only be used for the purpose of the investigation, with the general exception that Care Trust may act upon information that no employer or Trust could reasonably ignore.

12.1.9 Absent Staff and Email

The Care Trust reserves the right to open and review any emails addressed to an absent staff member in order to continue the business of the Care Trust. This may be enacted when staff members are sick or unexpectedly absent for sufficient amount of time that the business function that the absent staff performs for the Care Trust is put at risk. Line management must provide written permission to staff members filling in for the absent person, and for the replacement staff member to observe common courtesy and confidentiality of the emails opened. Disciplinary or Dismissal procedures may be brought upon those staff and their line management who do not take reasonable steps to respect the privacy and confidentiality of absent staff members.

12.1.10 Requesting Monitoring and Interception

Both a staff member and line management can request monitoring to take place of the staff members' Internet and Email. In both cases the request must state:

- Reasons for the monitoring
- Usage of the information to be collected
- Person responsible for the information once collected

Interception cannot be requested on a casual basis. Interception may only be used in situations where serious unlawful or criminal activity is suspected, such

that it outweighs the necessity for confidentiality and privacy.
The Care Trust will consider Monitoring or Interception requests from 3rd parties, but will not be obliged to them unless there is a statutory or legal reason to be. The Care Trust will not be held by contracts with 3rd parties which request monitoring unless statutory or legal obligation exists.

12.1.11 Authorising Monitoring, Interception and Blockage

Monitoring and Interception may only be authorised by senior management with the authority to make decisions on behalf of the Care Trust in this regard. In practicality, this will mean only those at a Director level may authorise monitoring or interception. Authorisation to block inappropriate sites and email addresses is given to the IT departments on behalf of the Care Trust, however staff and line management, with the staff member's consent, may make requests to block certain sites or emails.

12.1.12 Levels and usage of Privacy and Confidentiality for Information

The Care Trust, in the course of monitoring, investigating and investigations, will attempt to preserve the privacy and confidentiality of its staff and public. In doing so it will attempt to collect and use the minimal information necessary to perform the action.
Specifically for Email this will entail a graduation of information in relation to privacy and confidentiality. In descending order of least private/confidential to most private/confidential:

- Sender's address, Date/Time Sent/Received
- Title or Subject Line
- Body of Email and any attachments

Activities will assess what the minimal amount of information needed will be and only collect and use that minimal amount.

12.1.13 Points to consider and records in a justification

The Care Trust is required to have defensible justification to instigate Monitoring, Interceptions, Investigations and to a lesser extent, Blocking. Such justifications should include all or some of the following areas:

- Benefits of the chosen monitoring method
- Weight of benefits vs. adverse impact to confidentiality, privacy and trust
- Alternative monitoring methods considered
- How intrusion has been minimised, in justification to the purpose
- What risks are being addressed for the Care Trust or Public
- Results of consultations (and if applicable, consent seeking) with worker, trade representatives, etc…
- Specify the type and purpose of information collected

The emphasis of justifications should be on the need to be fair to individual staff, therefore justifying to all staff and not just the one to be monitored or the particular situation being monitored (i.e.: Fairness to all or fairness to none).

12.1.14 Record Keeping regarding Staff Specific Monitoring, Interceptions, Investigations, Blocking

The Care Trust will keep permanent records of all justifications, decisions and criteria regarding staff specific Monitoring, Interceptions, Investigations and Blocking. These records will become part of the employee record of said staff unless it is otherwise inappropriate to the purpose of the activity. Any such information collected during a Monitoring, Interception, Investigation or Blocking exercise will be treated in accordance with the Data Protection Act 1998.

13 Appendix Nine – Freedom of Information and Data Protection Guidance

13.1 Specific Notice regarding Freedom of Information and Data Protection

The Care Trust and its staff should be aware that any information collected about Internet or Email usage, as well as any Emails written or received by the Care Trust or its staff may be accessible under the Freedom of Information Act 2000 or Data Protection Act 1998.
Although unlikely, it is possible that individual usage of the Internet could also become public knowledge. In particular the more senior a member of the Care Trust (with seniority equalling the individual's greater representation as the Care Trust), the more likely that the Freedom of Information Act will have the ability to gain access to their individual information.
Emails are particular susceptible to the Freedom of Information and Data Protection Acts. The Care Trust and its staff should be aware that Emails are considered legal documents and records, and as such represent decisions and opinions of the Care Trust. This will likely necessitate the Care Trust searching emails for relevant information requested by a member of the public about themselves, or a decision or record made by the Care Trust. Staff should be aware that the Care Trust could keep all emails in an archive over which they have no access to delete or modify their emails after being sent or received.

13.1.1 Ensuring Confidentiality and Privacy

The use of the Care Trust's email system cannot ensure the privacy or confidentiality of communication. Therefore should a staff member, or member of the public, wish to ensure that the information they are providing or discussion they are having has a greater level of confidentiality and privacy, they should use the postal services available to them. Where it is not possible or practical to use the postal service staff members and members of the public should review the statements below.

13.1.2 Care Trust and staff responsibility for confidential/private emails

The Care Trust will expect that if an email is private/confidential it will be so marked. Staff should be aware that if emails are not so marked, the Care Trust may not have reason to suspect there is private or confidential material within and may open it without using Data Protection protocols appropriate to the handling of confidential information.
Where an email is marked private/confidential, the Care Trust will attempt, where appropriate, to preserve the confidential/private nature of the email during any investigation or monitoring activities.

13.1.3 Generic or Unit Accounts

An Email account that sends and receives emails from a generic clinical or business may be monitored without consent of any staff as the account exists as a business unit of the Care Trust. Staff should be aware that this account does not have the usual protections of the Data Protection Act or privacy and confidentiality for staff (although it does for the public), as it is not an account associated directly with a named staff member and therefore should never be used for any type of personal use.

13.1.4 Shared, Named Email Accounts

Where staff share an inbox that is a named inbox of a single staff member, reasonable steps should be taken to alert potential senders of email that emails sent to that account might be viewed by person(s) other than the account owner.
In practicality it would be sufficient to place a notice in the email of the named people who may also have access to the email account. This may be done automatically as part of a signature. Alternatively websites or other literature providing this kind of shared email address should advertise that it is not an account accessed solely by the named person.
Where confidential or private information is to be sent to one of the account viewers, the sender should include a note in the title indicating who may read the email, and the Care Trust will have reasonable expectations that this request is adhered too.

13.1.5 Forwarding Confidential Email

The Care Trust respects emails as legitimate records and documents. It therefore expects the same level of confidentiality and security for email to be adhered to as though it were any other confidential material. Forwarding confidential emails therefore would have the same consent issues as any other piece of confidential information.

13.1.6 Sending Confidential Information Outside of the Care Trust Network

The Care Trust strictly forbids the transfer of confidential information using email, or as attachments in emails, to organisations outside the Care Trust without it being encrypted, password protected or otherwise protected. Staff should therefore take care when including patient names or confidential situations or data in the body of an email to ensure that it is not being sent outside the Care Trust and has a confidential identifier on it.
Usually the easiest method to protect information is to create it on a MS Office document then password protect the document prior to sending it. Obviously it would not be advisable to send the password on the same email, or any other email within close timing of the first. Generally it would be recommended to provide such passwords using the telephone or a different communications technology.

14 Dissemination and Implementation of the Guideline/ Policy

<To be completed>

- How will the policy/ guidelines be presented/launched/introduced in the clinical area?
- How will training or education needs be identified and met
- Will there be someone to contact for clarification or support in the implementation of the policy
- Is there a clearly defined audit mechanism?
- How will the audit feedback be conveyed back to the staff implementing the policy?

15 Review

Date/Trigger	Review Areas
Time Independent Reviews	
Changes to the Data Protection Act 1998	Information Collection and Retention Areas
Changes to the Lawful Business Practice Regulations 2000 and Investigatory Powers Act 2000	Monitoring and Interception Areas
Significant changes in Care Trust technology (e.g. Implementation of NHS mail)	Affected Areas
Changes to Care Trust interest in providing the personal use of the Internet and Email	Affected areas, principles, guidance questions and/or entire policy
Timed Reviews	
Post-Consultation tweaking. Expected 12/04 – 02/05	All applicable areas
Yearly Review, Dec every year	All applicable areas

POLICY FEEDBACK FORM

POLICY TITLE	
POLICY REFERENCE	
DATE FOR REVIEW	
DATE FOR COMMENTS	

COMMENTS/SUGGESTIONS FOR POLICY REVIEW:
Areas to consider: local service developments, impact of policy on practice,