Camden and Islington NHS
Mental Health and Social Care Trust

Internet and E-Mail Policy Manager's Guide

Version 1.0

Camden *supporting partnership in mental health* ISLINGTON

Introduction

Health and Social Care requires a great deal of communication and in the modern NHS we are fortunate enough to have the Internet and Email amongst our communication tools. It is important to remember however that these tools must be used effectively and responsibly. As a staff member of the Care Trust you are responsible for your own usage of these tools as well as the usage of the staff members you directly manage. This guidance is to help you protect the Care Trust and your staff from misuse of these tools.

This guidance is created from the Care Trust's Internet and Email Policy, in particular Appendices 2 (Management Responsibilities and Guidance) and 5 (Appropriate Usage Guidance and Mis-usage)

Summary of Managers Responsibilities for Internet and Email

Managers (be it team leaders, service managers or directors) are responsible for the usage of the Internet and Email by the staff that they directly manage. The responsibility includes:

- ❑ To have read, understand and agree to the terms and directives of this Guidance.
- ❑ Judge whether to granting personal usage of the Internet and Email on the basis of minimal risk to their staff and Care Trust business.
- ❑ Provide permission for the personal use of the Internet and Email without prejudice or bias.
- ❑ Prior to allowing staff personal usage of the Internet and Email, have read, understood, signed and dated their staff's personal usage declaration, and ensured that this declaration is sent to the appropriate person
- ❑ Actively managing the risks of staff mis-using the Internet and Email
- ❑ Seek appropriate permissions to perform monitoring activity on their staff's usage of the Internet or Email from Care Trust Executive.
- ❑ Ensure that disciplinary and dismissal procedures relating to Internet and Email misuse are carried out fairly.

Staff with middle management responsibilities also have 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)
- ❑ Allow personal usage of the Internet and Email within their team(s) and service(s)

Granting the Personal Usage Privilege

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 business. Personal use of the Internet and Email should be considered and provided separately. The definition of the personal use can be found in Appendix Six of the Internet and Email Policy.

A Manager must provide a written documentation of having granted permission to the staff member. Any written permission will do, so long as it is acknowledged by both the manager and the staff member. A proforma is also available. It is also required for managers to document the justification for withholding or removing the privilege. The staff member, the manager and the manager's manager should keep all written documents relating to granting of personal use of the Internet and Email.

When considering granting personal usage of the Internet or Email managers should consider:

- ❑ Availability of computer resources
    - o 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?

- ❑ Ability to use the business tools
    - Staff that are unable to use the Internet or Email should not be allowed to use the Internet or Email until they have been given some training or demonstrate some ability to use them. It may be appropriate to provide staff with minimal training some personal usage in order to encourage their development with the business tools.
- ❑ Previous offences
    - It may not be suitable to grant personal usage to staff who have previously violated the Internet and Email Policy. Assess the risk of re-offence and whether the situation of the previous offence would present itself again. Remember! –Managers are responsible for the actions of their staff and may be subject to discipline and/or dismissal if they did not make reasonable efforts to ensure their staff use the business tools appropriately.
- ❑ Workload
    - Only if granting personal usage outside staff break periods should managers consider workload issues. For instance; 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 of the Internet and Email until such time as managers are satisfied they are able to use the business tools and are familiar with the relevant policies or guidelines. Managers have the duty to ensure that new staff are trained quickly so that they are not unduly denied the personal usage privilege. Remember! – New staff will need to have their Declarations signed before they are granted use of Email or Internet

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

- ❑ Performance of the employee
    - Staff are entitled to break periods regardless of their performance and what they chose to do during their break is not dictated by 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 full time 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.
- ❑ Management Circumstances
    - Personal usage for staff cannot be denied because managers are not aware how to, or are not interested in, monitoring the staff member's activity. Managers who are not comfortable with the technology must become familiar and comfortable with the technology. It would be acceptable to deny the privilege for a reasonably short period of time if managers are undergoing training to familiarise themselves with the business tools.

Timing of Personal Usage

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

Recommendations for the method of granting the Privilege of Personal Usage

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

Personal Usage and Internet Mail Specifics

If the staff member is granted personal usage of the Internet then it is acceptable for them to access their personal Internet mail services (e.g.: Hotmail, Yahoo Mail, etc…). Managers may not monitor the contents of staff's personal accounts on these services, however they must make staff aware that they should never be using these accounts for Care Trust business.

Internet Cafés

Note that all staff are able to use the computers supplied by the Internet Café at St. Pancras, St. Luke's and the Highgate Centre during their appropriate lunch break, regardless if they have been granted personal usage of the Internet or not.

Removal of the Personal Usage Privilege

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 staff member's usage would be considered inappropriate by the guidance here or in the Internet and Email 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

It is required that managers provide to staff written notification of the removal of the personal usage privilege and to forward the documentation, and justification for the removal of the privilege to their own manager.

Allowing Printing for Personal Use

Printing for personal reasons will be at the decision and explicit permission of the manager. Whenever possible the printer must be supplied with paper personally purchased by the staff wanting to print personal material. Care Trust paper is not for large personal printing requests and therefore cannot be bought from the Care Trust for this purpose or authorised for such use by the manager. Printing using the personal paper still costs the Care Trust money and resources; therefore managers should consider carefully the size and frequency of all personal printing 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 reasons 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, managers should carefully consider the size and frequency of those requests in regards to the cost or replacing colour cartridges for that printer.

Managers should encourage Staff to print double sided where it is appropriate and the printer can provide this.

Inappropriate approval of printing requests will be deemed as the manager's misuse and not the staff member's. Unauthorised use of the printer or Care Trust paper for personal use will be seen as misuse by the staff member and possibly by the manager if the Care Trust finds them to be negligent or complacent to the situation.

Defining Appropriate Usage

Managers do not have ability to define what is appropriate usage, but have the responsibility 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 of the Internet and Email Policy. In practice managers have the ability to define how their staff use the Internet or Email for business use only. Managers do not have the ability to define how the Internet or Email is to be used for personal reasons, other than to:

- Grant or deny the privilege of personal usage to their staff
- Monitor staffs' usage of the Internet and Business Tools, comparing their usage to the guidance offered here and in Appendix Five of the Internet and Email Policy
- Take action where staff usage is putting the Care Trust at risk, or the usage is not appropriate under the guidance given.

Monitoring Staff Usage of the Internet and Email using Reports

Managers are expected to actively monitor their staff's usage of the Internet and Email. Managers may receive reports of Internet and/or Email usage, which will not require permission to view or use from the Care Trust Executive.

Where the reports identify an individual and do not show any usage of the Internet or Email that would be significant, they should be destroyed.

Where the reports have activity of interest they should only be kept long enough for an investigation or similar to be completed and a decision made to engage in disciplinary or dismissal procedures.

Where the reports are used in any legal proceedings they should be kept as evidence until the legal case file is disposed of, otherwise all reports should be destroyed within a maximum limit of six months after their purpose has expired. Internet and Email activity reports should never become part of a staff's permanent personnel record.

Reports must be destroyed in such a way so that the identity of individuals cannot be discovered.

Remember – staff may have the right to see any information that we hold about them. When in doubt about whether staff can view their records, contact the Information Governance Manager.
The Information Governance Manager is contactable at:

Timothy d'Estrube
Information Governance Manager
Camden and Islington Mental Health and Social Care Trust
Room 111, 1st Floor, East Wing,
St Pancras Hospital
4 St Pancras Way
London, NW1 0PE

Phone: 020 7530 3019
Fax: 020 7530 3129
Email: timothy.d'estrube@candi.nhs.uk

Monitoring Staff Usage of the Internet and Email by other methods

Other monitoring activity can be part of proactive measures to ensure staff are using the Internet or Email appropriately but this will require Executive permission. For the following suggested monitoring activities managers must get written permission from their relevant Executive.

Intensive 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 guidance on this sort of monitoring of the Internet and Email is found in Appendix Eight of the Internet and Email Policy.

Managers are enabled and encouraged to use the following simple and minimal privacy invasive monitoring as part of their proactive measures to ensure compliance with proper use of the Internet and Email by their staff. These activities still require Executive or Staff member's consent which must be obtained prior to beginning the activities.

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 having casual titles and the times at which they were sent. Email sent to address that end in @yahoo.com, @hotmail.com or similar Internet 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 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, managers 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:

    - o Forwarding the emails as a batch to the next most senior manager, an executive or the Data Protection Officer
      This can be done 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.
      The Data Protection Officer is Timothy d'Estrube and can be contacted at:
      Timothy.d'estrube@candi.nhs.uk (020 7530 3019)

    - o 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 Window's "Search" function for key words relating to inappropriate material. The search function is found on the "Start" menu of the Window's desktop.
- ❑ 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 manager 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 or a decision was 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 of the Internet and Email Policy 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 of the Internet and Email may be legitimately removed during an investigation.

Dealing with Confiscated Material

Material confiscated by Managers should not be opened or reviewed until a review process has been worked out. This process needs to consider confidentiality of both the staff and the public against the necessity to investigate potential misuse. Such a process must receive agreement from an Executive member of the Care Trust. When in doubt of how to create such a process contact the Information Governance Manager or consult the Internet and Email Policy.

The Information Governance Manager is contactable at:

Timothy d'Estrube
Information Governance Manager
Camden and Islington Mental Health and Social Care Trust
Room 111, 1st Floor, East Wing,
St Pancras Hospital
4 St Pancras Way
London, NW1 0PE

Phone: 020 7530 3019
Fax: 020 7530 3129
Email: timothy.d'estrube@candi.nhs.uk

Usage and Mis-usage Guidance

The Care Trust understands that its staff are responsible and dependable employees and in this belief has given staff the ability to monitor their own behaviour on the Internet and Email. In giving staff this responsibility for their own usage the Care Trust has provided guidance in the form of questions as well as a list of definite mis-usage activities. Staff as well as their managers should use these questions to assess their usage of the business tools.
Use of the guidance questions depends on the "reasonable person principle". For staff and managers this means they must review usage of the Internet and Email through a summation or average of societal opinions and knowledge. This does not mean taking the opinion of an average person, but instead imagining as though they were looking at it as the collection of people who make up society.

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 managers make the decision, using the guidance given here, on what constitutes appropriate usage. Where staff and their 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. Management does not have discretion to define appropriate usage, only to interpret what the Care Trust has defined as appropriate usage.

When staff or their managers make decisions using the "reasonable person principle" they will be making judgements for which they are personally responsible. This responsibility will be linked to professional competency and therefore staff and managers may be disciplined or dismissed for poor judgement. 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 manager.

Guidance Questions One, for Business Usage

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

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

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. Where the answer is No, staff should not begin using the Internet or Email systems for that particular purpose. Where the answer is Yes, the staff should be assessed on the second question.

Guidance Questions Two, for Business Usage

The second Question asks if it is the appropriate and best usage of these business tools. Therefore staff should be assess on:

"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 appropriately. If the answer is No, then the staff will be justified in using the Internet or Email systems.
This question addresses staff's use the Internet or Email and the suitability of the use in the larger context of their responsibilities. This question is to help prioritise the usage of the Internet and the professionalism by which an email is written. It is an all-encompassing concept, but should be fairly easy to assess. Simple guidance to consider is:

- ❑ Multiple duties

    - If staff's 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 being looked 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.

Guidance Questions Three, for Business Usage

Question three relates to how a staff member uses Internet and Email. Therefore staff should be assessed on:

<u>"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?"</u>

Staff are expected to use the Internet and Email in a professional way, so that they and the Care Trust retain a professional respectability. 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, 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 staff write or respond to appear to the recipient or to the public? If staff allow emails to come to them from colleagues, or create emails, that if taken out of the context would not look like a professional conversation to the public it is probably inappropriate.
- ❑ Using Alternatives
    - If staff appear to be using the Internet or Email in an unprofessional way, despite having good reason to, but there are reasonable alternative way to accomplish the same goals without looking unprofessional then it is probably more appropriate to use the alternate method.

Using Guidance Questions during Personal Use

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 this guidance or the Internet and Email Policy:

Guidance Questions One, for Personal Usage

When engaging in the Privilege of person use, staff should be assessed on the following question:

<u>"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?"</u>

This question addresses 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.
    - o For instance, reviewing crude yet funny jokes is not likely to be appropriate.
- ❑ The "Child Test"
    - o 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.

Guidance Questions Two, for Personal Usage

Where the first question is Yes, staff should be assessed on the following second question:

<u>"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?"</u>

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
    - o If staff are using the Privilege, make sure that they are using it within the periods or constraints it has been supplied under
- ❑ Outside perceptions
    - o Would someone be able to reasonably make an issue over the staff's activities, for example consider if a report had a log of all the websites they accessed, would there reasonably be something to report in the interest of the public?

Specific Definitions of 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.

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. The Care Trust will apply these procedures under the Internet and Email policy, any other policy, or obligation (legal or otherwise) it may have in regards to the actions and materials held by the individuals involved. Managers are directly responsible for the actions of their staff they may face discipline or dismissal should the Care Trust find that inappropriate usage of the Internet and Email business tools has happened with their consent or support, or by their negligence.

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, managers 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, it would be prudent for managers to provide their staff member written permission for the material or actions to be taken.

The Care Trust strictly prohibits the downloading, uploading, transfer, processing, capture and storage of images, documents, media or executables using any of its systems for anything that is:

- ❑ Sexual Explicit
- ❑ Offensive, Derogatory and Defaming
- ❑ Trademarked or Copyrighted (without consent of the owner)

Individuals found to have violated this guidance and the Internet and Email policy will be subject to discipline and/or dismissal under general misuse of the Care Trust's business tools. This is 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 or the actions taken by the individual.

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 staff member they should note the site's addressing and method they arrived there, then immediately disengage from the site. Staff members should then report the sites address and the method arrived there to a Care Trust IT helpdesk, or failing that, their manager as soon as practical.
Note that sites that are not blocked by the Care Trust's processes are not by this characteristic considered acceptable sites. Sites that are obviously or borderline inappropriate sites that are accessible to staff should be reported to the IT helpdesk. Managers should monitor staff who have been found to have repeatedly visited an inappropriate but accessible sites and where necessary discipline or dismiss repeat offenders.

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 harmful software (e.g.: viruses)
- ❑ Intentionally disrupting network services (Care Trust or other)
- ❑ Distribution 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

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.

The Care Trust strictly prohibits the circumvention of its established network protocols and architecture without justified business reasons. In the case where a staff member has a justified business reason(s) to circumvent the established network protocols and/or architecture they must receive signed permission from the Care Trust's IT department/supplier and their managers. 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

(Those items marked with a "*" will be monitored by Care Trust IT and will not likely be a responsibility of less technically adept managers. Where misuse is thought to have occurred IT will contact the managers in question)

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. Staff found to have violated this policy will be subject to discipline and/or dismissal under general misuse of the Care Trust's business tools.