

CHRE

IT Code of Conduct

| | | |
|--|------------------|---|
| | Author(s) | Centre of Excellence |
| | Address | NorthgateArinso HR Outsourcing 239 Thorpe Park Peterborough PE3 6JY Telephone 01733 555777 Facsimile 01733 318849 |

Table of Contents

| | | |
|----------|--|-------------------------------------|
| <u>1</u> | <u>INTRODUCTION.....</u> | <u>3</u> |
| | 1.1 APPLICABILITY | 3 |
| | 1.2 RESPONSIBILITY | 3 |
| <u>2</u> | <u>PERSONAL USE</u> | <u>4</u> |
| | 2.1 PERSONAL USE OF CHRE FACILITIES AND THE INTERNET | 4 |
| | 2.2 PERMITTED PERSONAL USE | 4 |
| <u>3</u> | <u>MISUSE AND UNACCEPTABLE BEHAVIOUR</u> | <u>5</u> |
| | 3.1 ACCIDENTAL ACCESS..... | ERROR! BOOKMARK NOT DEFINED. |
| | 3.2 SENSITIVE DATA | 6 |
| <u>4</u> | <u>MONITORING & COMPLIANCE</u> | <u>8</u> |
| | 4.1 MONITORING | ERROR! BOOKMARK NOT DEFINED. |
| | 4.2 COMPLIANCE | 8 |



1 Introduction

The purpose of this Code is to provide guidance on the use of the Council for Healthcare Regulatory Excellence (CHRE) computer facilities, in particular the use of e-mail and the World Wide Web. It outlines our policy on the personal use of the IT facilities and gives guidelines on what use is not acceptable.

Used properly, these facilities can significantly assist CHRE in improving its business performance and also help in the development of staff IT skills. However, it is important that all employees behave responsibly when using these facilities.

1.1 Applicability

This code has been approved by the CHRE as part of their policy to open up access to the Internet. This document applies to all users of CHRE system's: this includes individuals seconded to CHRE and others who might transmit information across our system by means of e-mail or Internet services.

This code will apply to all CHRE staff as everyone has access to the Internet.

1.2 Responsibility

It is the responsibility of all users to comply with this Code. You must therefore ensure that you are familiar with its contents.

2 Personal Use

2.1 Personal Use of CHRE facilities and the Internet

The purpose of CHRE's IT facilities is to carry out tasks which support our objectives and goals. It is important that you understand that CHRE owns and is liable not only for the equipment and material, but also for any e-mails and downloaded Internet pages generated or stored on our equipment., Staff are however permitted to make limited personal use of the IT facilities in their own or outside normal working hours. Personal use must also conform with the minimum standards of conduct as set out in this Code and specifically in section 3.

2.2 Permitted Personal Use

You may use CHRE facilities to prepare simple documents or spreadsheets on personal matters (for example a letter to your bank or insurance organisation). Our registration under the Data Protection Act only covers information held on the system for work related purposes, so personal documents should only be stored temporarily on the system while they are being prepared, but must then be deleted.

You must not use CHRE facilities or the Internet to prepare or research material in connection with running a private business or use any other material which could be held to be of direct financial benefit to you or any third party connected to or known by you.

You may send brief personal e-mails with small attachments to internal and external addresses and you must use the message sensitivity option in Outlook to mark such e-mails as "personal". For guidance, brief e-mails should be no more than 10 lines of text and small attachments should not exceed 2 pages. Please discourage large incoming personal e-mails, particularly those with large attachments as these can clog up the mail gateway and stop work-related e-mails being delivered promptly. You must not use official templates for personal documents and private use of Chat Rooms and Newsgroups is not permitted. All e-mail activity is monitored, including personal e-mails. Disciplinary action will be taken against any member of staff who makes improper or excessive use of the e-mail facility (see Section 3).

If you are studying for any form of qualification, with the organisation's support, you may use the system to prepare study material. You must do this in your own time and ensure that you have the approval of your line manager.

Accessing the World Wide Web for personal purposes is also permitted provided that you do so in your own time and do not act in any of the ways described in Section 3 below. All Internet usage is monitored as outlined in Section 4 below. Line managers and the Chief Executive will be alerted and disciplinary action taken if there is cause for concern about attempted access to inappropriate sites or excessive personal time spent on the Internet.



3 Misuse and Unacceptable behaviour

If you misuse the system, you could be committing a criminal offence. E-mail is often spontaneous, which means that it can be written and issued without spending much time thinking about the content. However, if you make defamatory, actionable or untrue statements about colleagues or contacts on e-mail, this is no different from doing this in any other way. Such behaviour is likely to constitute a serious disciplinary offence and may also fall within the laws of libel. All messages must reflect the high professional standards to which CHRE subscribes. In addition, you must not seek at any time to access Internet sites that are clearly inappropriate.

A number of examples of what constitutes misuse of IT facilities, and what constitutes unacceptable behaviour are outlined below. This list is not exhaustive and each case is treated on its merits but any of these may, depending on circumstances, be treated as misconduct liable to disciplinary action. However, those in the first two bullet points below are more likely to be treated as serious disciplinary offences and could lead to dismissal for gross misconduct. It is recognised that there may be times where employees are required to view certain materials, as detailed below, in conjunction with their duties. It is essential in these situations that you obtain prior consent from the Chief Executive. Misconduct includes (but is not limited to) the following:

- Attempting to gain or actively gain access to an inappropriate Internet site and obtain or attempt to obtain pornographic or other offensive material (e.g. racist material) and generate, store, distribute, or display such material. This includes similar items on official laptops, palmtops or electronic diaries brought into the workplace. An inappropriate site and offensive material includes content of a sexually explicit or sexually orientated nature; material that would offend others on the basis of race, religion, colour, sex, disability, national origin or sexual orientation; and, material relating to illegal activities or activities otherwise prohibited.
- Acting in a way that compromises the safety of confidential and / or information e.g. by not following the information security policies, by attempting to gain access to such information to which you have no access rights, by sharing confidential and / or personal information with those who do not have access rights.
- Downloading any software on to any PC without the prior knowledge of the Office Manager who will advise whether or not this is suitable and whether CHRE IT consultants need to be involved.
- Subscribing to mailing lists ("listservers") through the Internet for purposes other than those that are work-related. This is to avoid unnecessary congestion of the e-mail system and consequent delays to the delivery of official e-mail.

- Attempting to obtain access to parts of CHRE network which you are not authorised to access is a criminal offence. Gaining such access with the intention of modifying data or programs is a more serious criminal offence.
- Generating messages in a way that makes them appear to have come from someone else.
- Sending messages that are abusive, offensive, libellous or can be deemed as harassment, bullying or a nuisance.
- Generating and/or distributing chain e-mail.
- Using the IT facilities for private commercial activity.
- Contravening rules for personal use of IT facilities.
- Disseminating or printing copyright materials in violation of copyright laws.
- Getting involved in user groups or discussions that are politically sensitive or potentially controversial.
- Using the Internet for political activity.
- Running a personal website.
- Private use of chat rooms and Newsgroups
- Improper use of official templates

Your CHRE system password should be kept secure at all times. It is recognised that there may be times when system access is required in which case there will be one individual, designated by the Chief Executive, who is able to gain full system access. There is no need to give anyone else your password. If you need to share data with colleagues, it should be stored in designated shared areas. Use the facility for delegating rights to your mailbox when away from the office.

3.1 Accidental Access

Internet users can connect accidentally to Web sites that contain illegal or offensive material. If this happens to you, you should disconnect from the site immediately and inform your line manager. If you receive an e-mail which you consider may contain pornographic or offensive material, you should close the document and advise your line manager.



3.2 Sensitive Data

Never send sensitive information in an external e-mail or over the Internet. If in doubt about whether material is regarded as sensitive, you should seek advice from your line manager.



4 Monitoring & Compliance

4.1 Monitoring

CHRE is responsible for monitoring the use of its IT systems to ensure that security standards are complied with and for compliance with this Code. All e-mail activity including traffic into or out of the organisation is logged on our servers and all internet browsing is recorded.

Software is installed on all desktop computers that records internet usage including the user name, the computer, dates and times of domains visited and URLs accessed as well as the browsing time spent on each site. This software enables CHRE to run reports on all internet usage.

CHRE's IT consultant runs a quarterly report which displays a summary of all the website domains that have been accessed by staff on a random day and the total browsing time spent on that site. This is reviewed by the Director of Governance & Operations to ascertain any inappropriate websites that may have been accessed.

Any possible cases of misuse will be drawn to the attention of the Chief Executive who will decide in consultation with line management what action to take, which may include invoking the CHRE Disciplinary Procedure. Attempts to access, active accessing, downloading and transmission of pornographic, racist and offensive material will be treated as gross misconduct that could lead to dismissal. In extreme cases it may be necessary to involve the police, if there is prima facie evidence that a criminal offence has been committed. If you accidentally visit an inappropriate site you should inform your line manager so that there is no misunderstanding at a later date.

We will not actively use the software to monitor the volume of use by individuals but reserve the right to do so should there be a concern about an individual's performance. You should, therefore, be aware that your use of the internet at work is not private.

If line managers are concerned about an individual's use of the internet, then usage of the system should be discussed with the person concerned, referring to the IT Code of Conduct for guidance. If this approach is not feasible or has already been explored with the individual then line managers can approach their own line manager or the Director of Governance and Operations to request investigation of the usage. Similarly if you believe that a colleague outside your responsibility is misusing the system, or that your PC has been misused, you should contact your line manager.

You should be aware that many Internet sites keep a record of visitors to the site for marketing purposes and that this record could become public. You will need to ensure that you do not visit any sites where such publicity could lead to embarrassment to CHRE.

4.2 Compliance

You are required to familiarise and fully comply with the Code. You will be deemed to agree to its terms including the monitoring arrangements unless you specifically write to the contrary to Chief Executive.

If you have any enquiries about this Code, please contact the Chief Executive.



Document Control

Version Control

Printed documents are uncontrolled. This document is only valid on the day it was printed.

| Version | Status | Description of Version | Date Completed |
|---------|--------|-------------------------------|----------------|
| 1.0 | agreed | IT Code of Conduct | 19/09/08 |
| 2.0 | | Section 4.1, Monitoring added | 28/9/10 |
| | | | |
| | | | |
| | | | |

Associated Documentation

| Version | Description of Documentation |
|---------|------------------------------|
| | |
| | |
| | |

Legal Disclaimer

Copyright © 2008 NorthgateArinso HR Outsourcing. All rights reserved.

All material contained in this document is confidential and proprietary information. The document and any attachments may be legally privileged. Dissemination, copying or other use of its content is strictly prohibited and may be unlawful. If you are not on the intended recipient(s) list, please inform NorthgateArinso HR Outsourcing. No contract may be construed from this document.

