STAFF POLICY ON DATA SECURITY AND CONFIDENTIALITY INCORPORATING CLEAN DESK STANDARD

DOCUMENT CONTROL

Document owner:	HR Manager
Approved by:	Senior Management Team (SMT) and DPO
Authorised by:	Senior Management Team (SMT) and DPO
Publication/circulation date:	10th June 2021
Planned review date:	10th June 2022

DOCUMENT REVIEW HISTORY

Document Reviewed and Amended (Y/N):	Y
Version Number:	Version 0.2
Document Location:	TBC

Content

1 STAFF POLICIES ON DATA SECURITY AND CONFIDENTIALITY

1.1 INTRODUCTION

This document sets out the procedures for observing confidentiality and security of data within the National Cancer Registry, Ireland (NCRI). It is meant to offer a series of principles, and cannot cover every possible eventuality. When in doubt in a situation which may involve confidential information, please contact the Director, who is the designated Data Controller under the Data Protection Acts, or in his/her absence a nominated responsible person. All staff are expected to make themselves familiar with the rules contained in this document, and to re-read them annually. A confidentiality statement is attached, and must be signed by each staff member on taking up his or her post and annually thereafter. **Any breach of these guidelines will be considered a serious disciplinary matter and may lead to dismissal.**

The Registry is in a position of trust. We are trusted by society at large and, in particular, by health care professionals, to observe the highest standards of security and confidentiality with regard to the very sensitive information which we have in our possession. We must also be aware of the disastrous consequences for the NCRI, should our sources of information lose their trust in us. The basic principle of operation of the Registry must be, above all, to protect the rights of the individual.

The rules set out here govern the handling of confidential or otherwise sensitive personal information. This is described as any information which could identify an individual (employee, patient, family or health care worker) either directly or indirectly. The fact that an individual is registered is in itself an item of confidential personal information. Individuals may be directly identified by name, address, date of birth or personal identification number (e.g. PPS number, medical record number), or indirectly through a unique combination of personal characteristics.

Apart from confidential personal information, the NCRI also produces statistical information on cancer. Many different individuals and groups may request this information. Because cancer incidence information is not always easily interpretable, the Registry needs to be able to control the uses made of information supplied by us, at least to the extent of having the users take responsibility for any interpretations. The Director must first clear all requests for restricted or confidential information, no matter how apparently innocuous. All data requests should be sent to data-requests@ncri.ie from website data request page and ncr info@ncri.ie from website 'contact us' page.

NCRI staff may, in the course of their work, come across information not pertaining to cancer registration, or may have access to confidential information on others which might be of interest to them. The same rules of confidentiality apply to personal information, whether gathered for registration purposes, or come across incidentally. Staff must not abuse their privileges of access to medical records by seeking information not relevant to their work.

1.2 DATA SECURITY

1.2.1 BASIC PRINCIPLES

All staff concerned with the collection, processing and output of personal data are employees of the National Cancer Registry. On taking up duty, and **annually thereafter**, they are required to

- read, agree to and observe the rules set out in "Staff Policy on Data Security and Confidentiality Incorporating Clean Desk Policy".
- sign an undertaking of confidentiality, which will remain binding even following their departure from NCRI work. This undertaking prohibits staff from disclosing, either directly or indirectly, to any individual outside the NCRI or to other staff within the NCRI who do not have access to confidential information, the identity of any

person registered, or any data concerning such an individual, or any other confidential material they may come across in the course of their work.

- To observe the security precautions currently operating within the NCRI.

1.2.2 PHYSICAL SECURITY

The operation of the NCRI is largely electronic, and few written or printed documents containing individual identification are created. Any such written documents are to be cross or confetti-shredded immediately after use. Documents which need to be kept for archival purposes are to be stored securely in locked storage cabinets. Access to these cabinets is limited to authorised NCRI personnel.

The NCRI door is to be kept locked at all times. Visitors to the NCRI must be admitted to the NCRI premises by a staff member. Once admitted they should remain in the outer lobby area until the person they are meeting arrives. It is the responsibility of the person first admitting them to the premises to ascertain who the visitor is, whom they are visiting and to ask them to remain in the lobby area. The person they are visiting must ensure they sign in to the visitors' book and sign out on departure, are given a visitor's badge, are accompanied at all times and have no access to areas where sensitive information which could include special categories of personal data could be visible. Unless there is a specific reason for doing otherwise, visitors should be confined to the non-secure areas of the NCRI (meeting rooms, lobby, Director's office).

The NCRI premises are protected by high-security locks and by electronic alarms. Non-NCRI staff must never be given alarm codes. It is the responsibility of every staff member to ensure that these are activated when the offices are unattended at any time. The last person leaving the premises every day should go through the standard "last person out" process and sign to indicate that the checklist has been followed.

Confidential documents should be on the desktop only when being used. At all other times they should be stored in a designated locked cabinet or drawer. Staff should observe a "clean desk" policy when working with confidential documents; all non-essential documents, whether confidential or otherwise, should be cleared away whenever the desk is unoccupied, even for brief periods (e.g. coffee breaks) to reduce the risk of inadvertent exposure of a confidential document. When printing documents the user should ensure that confidential documents are not left on printers – only print what is absolutely necessary.

1.2.3 ELECTRONIC SECURITY

Data collected by NCRI staff on laptop computers is password protected and encrypted. Data is stored on laptop computers in an encrypted format that would be quite difficult for the average person to break into. However, it is not impossible, with enough time, determination and technical skill. The loss or theft of a laptop computer with confidential data is one of the most serious potential threats to the NCRI and all staff are required to comply with the laptop security policy. Details of the NCRI's security policy specific to laptops are outlined in section 1.3, page 8. Staff should adhere strictly to the laptop security policy (Section 1.3.) If any breach of security is suspected, must be reported verbally to the responsible person immediately. The **responsible person** for each staff member is, in the first instance, their line manager. If they have no line manager, or the line manager is not available, a member of the Senior Management Team or the Director should be contacted. The Director will nominate someone to be responsible for data security in his/her absence

Password policies with regard to laptop password format and frequency of change must be complied with; and these are technically enforced by IT.

Data within the NCRI is protected by passwords and encryption. Each individual within the NCRI has a network password. This allows access to the NCRI network and approved systems. Password rules are technically enforced and all password policies must be complied with. Passwords must never be written down anywhere and must be encrypted if stored in electronic format. Access to the cancer registration system (ACES) also requires a valid, time-limited security certificate to be installed on the user laptop. ACES records reads of/changes to a registration, by whom and when. Access to all computers is automatically logged by the network system, which records the identity of the person using the computer, and the times at which they log on and log off. Staff must log off when leaving the NCRI, and not allow any identifiable data to appear on the screen while leaving their desk. Remote network access requires a valid, time-limited security certificate to be installed on the laptop. NCRI computers which contain, or which have network links to, personally identifiable data are not to be connected to any outside computer system unless IT have secured the connection and verified its security.

While regular backups of network data are made, each staff member has a responsibility to ensure that any data not held on the network is backed up. Where a staff member needs to download sensitive personal data, software is provided to ensure that data is deleted on shutdown. No sensitive personal data (whether identifiable or pseudonymised) should be stored locally.

1.2.3.1 PASSWORDS

Passwords are an important part of computer security. They are front line protection for user accounts. A poorly chosen password may result in a hacker breaking into the system. Appropriate steps must be taken to select and secure passwords. Password and user accounts must not be shared or used by anyone other than the designated user. Please refer to the Password Policy for further details.

1.2.3.2 ENCRYPTION SOFTWARE

All NCRI laptops are encrypted. This encryption mitigates against the unauthorised use of the laptop if it is lost or stolen.

1.2.3.3 REMOVABLE MEDIA DEVICES.

Removable media devices are any type of storage device that can be removed from a computer while the computer is still running, for example USB keys.

Removable media devices are conveniently small, portable and easy to use. However, these benefits also mean the device is easier to lose, misplace or have stolen.

The following are areas to consider when using any removable media device that contains NCRI data or data pertaining to the NCRI or cancer registration (- “data” in these points means data relating to individuals, living or deceased , regardless of the level of pseudonymisation involved, but generally not including aggregate tabulations etc. except where these are so finely broken down that they may risk disclosure of potentially sensitive information at an individual level).

- A removable media device should only be used when absolutely necessary and there isn’t an alternative way of transporting the data. In these cases, the device should contain only the minimum data required.
- Only devices issued or approved by the IT department can be used, this is a technical control. All other devices allow reading but prevent writing.
- It is essential that a removable media device is encrypted to an acceptable level. If you have any doubt or concern about the security of the device, please check with the IT department before using it.
- A removable media device should not have any external branding or labelling that identifies it as belonging to the NCRI or gives an indication of the nature of the data contained on it.

- When a removable media device is removed from the office, the user should be aware of any data that's on the device. If data is added to the device externally, this information should be noted.
- On returning to the office with a removable media device, any data should be transferred to the network as soon as possible. This transfer should include the removal of the data from the removable media device and return of the device to IT

1.2.3.4 FILESENDER

FileSender from HEANet, is used for the majority of patient-level datasets sent outside NCRI in response to approved requests for research, audit or administrative purposes.. To use Filesender, logon to FileSender using your NCRI network username and password and upload the file by filling out a form that sends an email to the person that needs to download the file. They will receive an email with a link to the file which is only available for a set time period before it is deleted from the HEAnet server. FileSender can be used from anywhere you have an internet connection. Although FileSender is a secure service any confidential patient data should be encrypted before sending.

It can also be used to allow external people to send in large files through the use of a "guest voucher" where they are sent an email with a time-limited option to upload a file.

1.2.3.5 HEALTHMAIL

Healthmail is a service that allows health care providers to send and receive clinical patient information in a secure manner. Healthmail is a service of the HSE and is supported by the Department of Health and the Irish College of General Practitioners. NRCI staff should refer to the available Healthmail Standard Operating Procedures.

The NCRI have signed up to Healthmail (ncri@healthmail.ie). It is safe to send patient identifiable clinical information between @healthmail.ie and @hse.ie or @voluntaryhospital.ie addresses. When exchanging data via Healthmail it is advisable to exchange a test e-mail as the initial exchange.

1.2.3.6 VIRUS PROTECTION

Anti-virus software is managed centrally by the IT Department and your laptop will automatically update in virus definitions.

WHAT TO DO IF YOU SUSPECT A VIRUS:

- Immediately stop using your laptop.
- Notify your IT department.
- Do not re-use your laptop without approval from IT.

1.2.4 SECURITY DURING DATA COLLECTION AND PROCESSING

a. The arrangements for security and confidentiality within each hospital must be strictly observed in addition to the NCRI policies and protocols.. Medical records should not be taken from areas assigned to them without the specific permission of a responsible hospital authority.

b. All confidential material must be stored out of sight when not personally attended.

c. Details of cases should be discussed only with the doctors responsible for the case; staff should not assume that others within the hospital are in possession of the same amount of information as they are.

d. Material that is not pertinent to NCRI work should never be examined.

e. Data received from other sources in physical format—memory key, CD, tape, printed reports etc. must be logged in on receipt, labelled, and kept in secure storage until used and then destroyed.

f. Where relevant NCRI staff should refer to the Handling Hardcopy Data external to NCRI Standard Operating Procedures.

g. All printed reports, records, questionnaires and interview records which contain identifiable data, should be treated with the same procedures as patient registrations and should never be left unattended in an open area. All printed material should be immediately retrieved from the printer area.

h. All printed records, questionnaires and interviews records with personal data should be shredded as soon as they are no longer needed.

i. When printing reports for internal use, avoid the use of identifiers, unless this is essential for the purpose of the report.

1.2.5 COMMUNICATION

1.2.5.1 EMAIL

a. The email system is intended for the business purposes of the NCRI reserves the right to curtail or prohibit all, or specific, personal usage.

b. When forwarding emails it is important to check for sensitive, inappropriate or confidential information in the message being forwarded.

c. Please refer to the General Principles section to find information about acceptable email use.

1.2.5.2 TELEPHONE

a. Information concerning identifiable patients or research subjects should **never** be given over the telephone to non-NCRI staff without written permission from the patient.

b. Calls to medical or para-medical staff concerning registered patients or research subjects should use the minimum of detail essential for the person being called to identify the patient (e.g. medical record number, date of birth rather than name and address).

c. If there is any possibility that confidential information might be overheard in the general office, use the designated soundproof rooms.

d. Staff using offices shared with non-NCRI staff should not discuss confidential information if the office is occupied.

e. Calls from persons identifying themselves as cancer patients and asking for information should be dealt with in a way which does not disclose if the individual is registered or not. Once the person has identified themselves, the enquiry may be dealt with by

    a. Asking that the person write in for information which can be sent directly, or to a named medical practitioner

    b. Asking permission to telephone the person's GP with the information.

Please refer to the Subject Access Request Procedure for more information.

On occasion, family members of patients may contact the NCRI, usually after receipt of a letter asking the patient to take part in a research study. It should not be assumed that the person calling has any knowledge of the patient's condition, or that they are acting with the patient's express consent. The response to the call must not reveal if the patient has cancer.

1.2.5.3 LETTERS

a. All letters to consultants, general practitioners, patients or research subjects which contain confidential information on living individuals should be addressed to them personally and marked "Confidential" and mailed by registered post. If you are unsure of the person to whom you should address the letter, please confirm their

name and address by telephone before writing. If confidential information is sent out, and you cannot be certain that this will reach the recipient, check its arrival with the recipient by telephone.

b. Any communication between NCRI staff with regard to patients should use patients' registration numbers, not names and/or addresses, or should refer to files stored in secure network locations to which only specific staff have access. Material should be sent electronically and encrypted, rather than by post, if possible.

1.2.5.4 Video Conferencing & Instant messaging

The NCRI use Skype for Business for an instant messaging and video conferencing solution. The system is implemented onsite. Communication is limited to only NCRI users. To use the system, you must first be connected to the network via GlobalProtect.

- All communication is encrypted and cannot be viewed by anyone outside of the conversation/ video call. The content of any messaging or video is not persisted. Once you close the message window and/or video window, there is no record of the content stored. A log is kept that a conversation took place and the date and time, but no more information than that. In practice, if a business decision is made over Skype, you should follow this up with a persisted record, e.g. email or document saved on the network.
- For security purposes, you should treat all communication through Skype for Business in the same way as you do for telephone conversations.
- The functionality to share your desktop with others has been removed as has the functionality to share files over Skype. If multiple parties on a Skype call require a file for reference, you will need to distribute via some other means, e.g. a link to a network file.
- For those users using a HP laptop, the inbuilt camera can be used for video conferencing. For those using a Dell laptop, you require an external webcam.

Please refer to the NCRI Skype for Business User and the Skype for Business Meeting Set-up Guides for further information on operation and security settings.

1.3 Laptop Security Policy

1.3.1 Purpose

This policy addresses the actions that must be taken by all NCRI staff who have an NCRI laptop.

1.3.2 Requirements

All laptops acquired for, or on behalf of, the NCRI shall be deemed to be the property of that organisation. Each employee issued with a laptop is responsible for the security of that laptop, regardless of whether the laptop is used in the office, at the employee's place of residence, or in any location such as a hotel, conference room, car, train or airport. (Note: This list of potential places is not exhaustive.)

If, for any reason, you find that you cannot comply with the NCRI policy on storage and transport of your laptop, your line manager and the IT department must be informed and alternative arrangements approved.

1.3.3 Storage and transport outside the main NCRI offices

For the purposes of clarity, in situations where an employee is working from home, their locked house is considered the same as a locked room. If the employee leaves their laptop in the NCRI office this is also considered the equivalent of a locked room.

- At the end of the working day the laptop should be placed in a locked cabinet or room. If this is not feasible, alternative secure arrangements must be agreed with the Director.
- The laptop should always be stored and transported in its carrying case.
- While travelling by car the laptop must be stored in the boot and secured against movement.
- While travelling, keep the laptop and laptop peripheral equipment with you.
- When taking annual leave make sure the laptop is securely locked away in a locked cabinet either in the NCRI offices or (for Cancer Data Registrars) in the base office or the employees external base workspace. If you are unable to do this IT must be notified.
- Unaccompanied shipment of laptops to and from the NCRI must be arranged by, or with the approval of, the IT department, using an approved courier. Please refer to the Laptop Dispatch and Return Standard Operating Procedure.

1.3.4 Laptop usage outside NCRI offices

- Laptops should be used **only** for NCRI work.
- Software should be installed only with IT approval.
- If you encounter problems with the laptop, do NOT attempt to repair it yourself. Do not have anyone not pre-approved by IT attempt to repair the laptop.
- When away from the laptop temporarily during working hours the laptop must be electronically locked using the Windows 10 locking functionality or the Windows + L command. Where possible attach Kensington lock supplied by NCRI as additional security measure.
- If you need to leave the office disconnect from the NCRI's network and from the internet. If using a mobile wi-fi device (dongle) to connect to the internet, store it in a secure place if possible or bring it with you.
- The laptop display should be positioned to preclude casual viewing by others (as far as is reasonably practicable), especially when confidential data is shown on the display.
- When NCRI staff use a laptop to connect to the NCRI server in Cork, they should connect only to systems they are authorised to use. NCRI staff should always log off the NCRI server during periods of inactivity.
- IT require that staff firstly connect to the internet and then immediately connect to the network via VPN software. This means they are connected to NCRI servers. If a user is disconnecting from VPN software, they should be cutting off their internet access also.

1.3.5 Violation and Penalties

- Employees should comply with this policy as far as reasonably possible. If you feel you cannot comply with or do not fully understand this policy please contact the IT Department or the Data Protection Officer.
- Unreasonable violation of this policy may be grounds for disciplinary action.

1.3.6 Collection of personal and sensitive information

Personal and sensitive information is collected by Human Resources (HR) only where it is necessary for the HR function or any related activity. This information will normally be gathered directly from the individual concerned. At the time the information is collected the staff member will be advised whether or not the provision of the information is compulsory. One example of this is the information collected through the disability census each year.

HR staff try to ensure that personal and sensitive information collected is accurate, relevant, up-to-date, complete and not misleading and will take all reasonable steps to protect these records from misuse, loss, unauthorised access, modification or disclosure.

1.3.6.1 STORAGE OF PERSONAL EMPLOYEE INFORMATION

Only staff members who require such information in order to carry out their duties and responsibilities will have permission to access personnel files. Electronic access to the Human Resource Information System is restricted to staff who have direct responsibility in that area and the system is password protected. Hard copies of employee personnel files are stored in locked cabinets and access to this area is restricted to HR staff.

1.3.6.2 USE AND DISCLOSURE OF PERSONAL EMPLOYEE INFORMATION

HR staff must not disclose personal information unnecessarily. Sensitive information can be disclosed only with consent. Protection of confidentiality includes ensuring files and work areas are organised so that information is not inadvertently disclosed. Staff must only access information that they require for legitimate work purposes.

1.3.6.3 HUMAN RESOURCES STAFF–PROTECTING THE PRIVACY OF EMPLOYEES

The following are practical, everyday work practices that HR staff should apply in ensuring confidentiality in the workplace.

- When temporarily away from workstations during working hours HR staff must electronically lock their computer or use an automatic screensaver lock.
- Filing cabinets or drawers containing confidential information located at individual work stations are to be locked when not in use and when the staff member is away from their workstation
- HR staff members should maintain awareness when having confidential telephone conversations, or impromptu meetings at their desks
- There should be no discussion of any matter relating to sensitive staff information in social environments
- Printed information should be collected promptly from shared printers and photocopiers
- Confidential information that must be retained should be archived. If the information is no longer required it should be shredded.

1.4 BREACHES OF DATA SECURITY OR CONFIDENTIALITY

1.4.1 LOSS OR DISCLOSURE OF CONFIDENTIAL DATA

1.4.1.1 PROCEDURES BY THE PERSON HOLDING THE DATA OR BECOMING AWARE OF THE BREACH

1. All breaches of confidentiality, or suspected breaches, must be reported verbally to the responsible person immediately. The **responsible person** for each staff member is, in the first instance, their line manager. If they have no line manager, or the line manager is not available, a member of the Senior Management Team or the Director should be contacted. The Director will nominate someone to be responsible for data security in his/her absence.
2. An initial assessment of the alleged incident should be carried out and if a breach of confidentiality is confirmed, the DPO should be notified and a report should be compiled without undue delay.
3. The resulting report should include a clear description of the data lost or revealed, the date, time and the circumstances under which this occurred and measures taken, if any, to retrieve the data. It should be followed by a written report with the same information in more detail and giving details of the procedures which should have applied and why these were either not followed or proved inadequate.
4. The report should note if any other persons have been informed, or need to be informed (e.g. hospital management, Garda, Data Protection Commissioner). If any of these need to be informed this should be done by the responsible person.
5. If data has been lost or mislaid and it can possibly be retrieved before it is read by anyone outside the NCRI then every possible step should be taken to retrieve it; however, successful retrieval of the information does not remove the obligation to inform the responsible person.
6. If data has been misdirected (e.g. through post or email) the person to whom it was mistakenly sent should be contacted immediately, informed of the confidential nature of the data and asked to destroy it unread.

1.4.1.2 PROCEDURES FOR THE RESPONSIBLE PERSON

1. If it is suspected that confidential data has been disclosed, initiate procedures in the Data Breach Policy.
2. All breaches of confidentiality, or suspected breaches, must be reported to the Director, or in his/her absence a nominated responsible person, as soon as possible.
3. Risk assessment should be carried out—
    a. what type of data is involved, has it been lost or disclosed, to whom, is this NCRI or third party (e.g. pathology report) information?
    b. Has there been a breach of procedure? If so, the disciplinary policy may be utilised.

1.4.2 BREACHES OF SECURITY PROCEDURES

1. Breaches of data security should be reported by anyone becoming aware of these.
2. A log of all breaches will be maintained by the DPO.
3. The Director, or in his/her absence a nominated responsible person, should be informed of any breach as soon as is reasonably possible.
4. Breaches of security may be followed by disciplinary procedures including verbal and written warnings, entries in the individual's personnel file, suspension or dismissal.

1.5 Internet, Network and Email Policy

1.5.1 Introduction

The National Cancer Registry, Ireland (NCRI) aims to provide you with accessible, up-to-date and reliable information to support you in your work. This goal requires the NCRI to provide access to the information resources of the Internet to help you do your job and be well-informed. The Internet is a business and research tool for NCRI. Users must understand that any connection to the Internet offers an opportunity for non-authorised users to view or access corporate information. Therefore, it is important that all connections be secure, controlled, **and** monitored to provide you with accessible, up-to-date and reliable information and learning technology to support NCRI activities. Users must not attempt to bypass any of the NCRI's security features. The NCRI reserves the right to block unacceptable content that may be dangerous to the network

1.5.2 General Internet Use

1.5.2.1 User accountability

Users are responsible for their network use (including Internet use) and are accountable for their own work.

1.5.2.2 Virus Detection

All files obtained from sources outside the organisation, or downloaded over the Internet are automatically scanned by virus checking software. However, if you suspect that a virus has been introduced into the NCRI network, notify the IT group immediately. If you suspect that an email may not be from a bona fide source (based on email address, your knowledge of the claimed sender or aspects of the content or layout of the email), do not open any attachment or click any links in the email, and contact IT for advice.

1.5.2.3 Unacceptable Content

The following content has been deemed to be unacceptable:

- Words, images or references that could be viewed as libellous, offensive, harassing, illegal, discriminatory, or otherwise offensive.
- Words, images or references that might be considered inappropriate in the workplace, including, but not limited to, messages or images that are lewd, obscene, sexually explicit, or pornographic.
- Words, images or references that might be considered inappropriate, harassing or offensive due to their reference to race, sex, age, sexual orientation, marital preference, religion, national origin, physical or mental disability, or other protected status.

1.5.2.4 Prohibited Activity

- Intentionally downloading, copying or transmitting documents or software protected by third party copyrights in violation of those copyrights. Any individual with a question concerning a copyright issue should contact HR.
- Viewing content that is illegal or unacceptable over the Internet or any other network.
- Creating or transmitting works containing illegal or unacceptable content over the Internet or any other network.
- Using encryption devices that have not been expressly approved by the NCRI.
- Using software that transmits and receives content over a network which has not been expressly approved by the NCRI. A list of acceptable software is available from IT.

- Storing works containing unacceptable or illegal content either locally or on any other machine on a network administered by the NCRI.

1.5.2.5 Accidental/Unintended Violations

If you find yourself accidentally viewing illegal or unacceptable content over a network as outlined above you must cease viewing the content immediately, regardless of whether that content provided had been previously deemed acceptable by any screening or rating program. A user who accidentally views unacceptable content over a network is encouraged to report the incident to the organisation's IT department without the threat of incurring a violation penalty.

1.5.3 Email

This sets forth the policy of NCRI with respect to email & internet usage. All individuals (including but not limited to staff, outside consultants and visitors) who use the NCRI email system (mail.ncri.ie) are required to comply with this policy statement. As email is transmitted over a network all conditions described in the previous sections apply.

1.5.3.1 General Principles

Acceptable use

- The email system is intended for the business purposes of the NCRI. The email account is not intended for personal use (see Internet and email policy) but limited personal use is acceptable. However, the NCRI reserves the right to curtail or prohibit all, or specific, personal usage.
- When forwarding emails it is important to check for sensitive, inappropriate or confidential information in the message being forwarded.
- No person identifiable information should be contained in an email subject line.

Ownership

All email accounts and all information and messages that are created, sent, received or stored on the NCRI email system are the sole property of the NCRI and are not the property of the employee or other individuals.

1.5.3.2 Email Review

All email is subject to the right of the NCRI to monitor, access, read, delete, copy, and use such email without prior notice to the originators and recipients of such email. Email may be monitored and read by authorised individuals on behalf of the NCRI for any violations of law, breaches of NCRI policies, communications harmful to the NCRI, or for any other reason. NCRI also reserves the right to disclose emails to authorised persons.

1.5.3.3 Email Content

Emails should be professional, courteous and in compliance with all applicable laws and NCRI policies. Emails should not contain unacceptable content. Users should employ spell check on all emails sent.

1.5.3.4 Security

The email system is only to be used by authorised individuals. Individuals shall not disclose their username or passwords to others and may not use someone else's username or password without express written authorisation from an authorised IT staff member.

1.5.4 Implications of the Freedom of Information (FOI and Data Protection (DP) Acts)

It is reasonable to assume that some of the information that may be requested under the FOI or Data Protection Acts will only be available in email format and more than likely be stored in an individual's personal email account. It is

essential that emails are appropriately filed and easily retrievable. Where information is stored only in email format, it is important that individuals are aware, so that emails are not deleted inappropriately.

The Freedom of Information and Data Protection Acts cover all information, not just formal documents. Therefore any individual's work-related emails can effectively become public property under the Freedom of Information Act. It is essential that Individuals know exactly what emails they have sent or received and when to delete them (i.e. when they are no longer needed). The following should help users make this decision themselves.

1.5.4.1 WHAT IS A RECORD?

A record is 'information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business activity'.

This definition was taken from – International Standards Organisation ISO 15489 Information and documentation: Records management, Part 1 2001.

1.5.4.2 IDENTIFYING EMAIL RECORDS

Email messages that might constitute a record are likely to contain information relating to business transactions that have or are going to take place, decisions taken in relation to the business transaction or any discussion that took place in relation to the transaction. For example, during the decision to put out a tender document for a particular service, background discussion about what this should and should not include might take place via email and should be captured as a record.

1.5.4.3 EMAIL RETENTION POLICIES

Users must retain copies of email records for inspection under the Freedom of Information Act. At present there is **no maximum limit** on a time for which an email record must be retained.

1.5.4.4 WHO IS RESPONSIBLE FOR ELECTRONIC RECORDS?

As email messages can be sent to multiple recipients there are specific guidelines to indicate who is responsible for capturing an email as a record:

- For internal email messages, the sender of an email message, or initiator of an email dialogue that forms a string of email messages
- For messages sent externally, the sender of the email message
- For external messages received by one person, the recipient
- For external messages received by more than one person, the person responsible for the area of work relating to the message. If this is not clear it may be necessary to clarify who this is with the other people who have received the message.

1.5.4.5 WHEN TO CAPTURE EMAIL AS RECORDS

Many email messages will form part of an email conversation string. When this happens it is not necessary to capture each new part of the conversation, i.e. every reply separately. There is no need to wait until the end of the conversation before capturing the email string as several discussions may have been covered. Email strings should be captured at significant points during the conversation rather than waiting until the end of the conversation.

1.5.4.6 WHERE TO KEEP EMAIL RECORDS

Email messages are automatically stored on the Microsoft Exchange email server, and are regularly backed up. So long as you use email in the standard way, all your messages will be stored. Messages you delete will be stored for 30 days after deletion.

1.5.4.7 MANAGING EMAIL RECORDS WITH ATTACHMENTS

The decision on whether an email and/or its attachment constitute a record depends on the context within which they were received. There are circumstances where the attachment would require further work in which case it would be acceptable to capture the email and the attachment together as a record and keep a copy of the attachment in another location to be worked on. In these circumstances the copy that was worked on will become a completely separate record.

1.5.5 DISCLAIMERS

A disclaimer is appended to all outgoing messages from an NCRI e-mail account, where the recipient is external to the NCRI.

E-mail signatures are applied to all NCRI e-mail accounts. This signature comprises the NCRI logo, user's name, job title, contact details and a link to the NCRI website.

Emails originating outside the NCRI are prepended with a warning message to the recipient to be sure of the legitimacy of the source before opening any link or attachment. When sending out a message in response to a request for data or general information, the user must append the following disclaimer themselves.

Cancer registration is a dynamic process and information is continually updated on our database. As a result, the figures given here may not correspond exactly to those in previous reports, or to those on our website.

1.6 VIOLATIONS AND REPORTING

Violations will be reviewed on a case-by-case basis. If it is determined that a user has violated one or more use regulations, standard disciplinary procedures will apply.

The NCRI intends to enforce this policy, but reserves the right to change it at any time as circumstances may require.

1.7 CLEAN DESK STANDARD

Every work space should have minimal materials visible and only those in current use, with the exception of any published (unrestricted) reports/references materials stored on shelves. No restricted materials should be left in plain view. Restricted materials are those (electronic or paper) stamped red, amber, strictly confidential and confidential or containing any personal data. When leaving the workspace for brief periods (less than 10 minutes) all restricted materials should be placed in a drawer and/or minimally concealed (e.g. turned over, monitor/screen locked). All restricted materials must be safely locked away and out of view when leaving the workspace for longer periods of time and at end of the workday. Staff are encouraged to keep a tidy workplace and to stamp all materials whenever possible.

Data confidentiality in the National Cancer Registry.

General policy, procedures for release of data and staff guidelines.

STAFF UNDERTAKING

All staff are to sign this undertaking annually.

I have read, and will abide by, this policy. I understand that any breach of this policy is a serious disciplinary matter.

Signed: _____ Date: _____

Name in block capitals: _____