

Staff Policy On Data Security And Confidentiality

|  |  |
| --- | --- |
| Version | 1.0 |
| Revision date | 01/03/2016 |
| Revised by | Harry Comber |
| Date approved by Board |  |

Contents

[1 Staff policies on data security and confidentiality 1](#_Toc444528051)

[1.1 Introduction. 1](#_Toc444528052)

[1.2 Data security 1](#_Toc444528053)

[1.2.1 basic principles 1](#_Toc444528054)

[1.2.2 Physical security 2](#_Toc444528055)

[1.2.3 Electronic security 2](#_Toc444528056)

[1.2.4 Security during data collection and processing 5](#_Toc444528057)

[1.2.5 Communication 5](#_Toc444528058)

[1.3 Laptop Security Policy 6](#_Toc444528059)

[1.3.1 Purpose 6](#_Toc444528060)

[1.3.2 Requirements 6](#_Toc444528061)

[1.3.3 Storage and transport outside the main Registry offices 7](#_Toc444528062)

[1.3.4 Laptop usage outside Registry offices 7](#_Toc444528063)

[1.3.5 Violation and Penalties 7](#_Toc444528064)

[1.4 Breaches of data security or confidentiality 8](#_Toc444528065)

[1.4.1 Loss or disclosure of confidential data 8](#_Toc444528066)

[1.4.2 Breaches of security procedures 8](#_Toc444528067)

[1.5 Internet, Network and Email Policy 9](#_Toc444528068)

[1.5.1 Introduction 9](#_Toc444528069)

[1.5.2 General Internet Use 9](#_Toc444528070)

[1.5.3 Email 10](#_Toc444528071)

[1.5.4 Implications of the Freedom of Information (FOI and Data Protection (DP) Acts 11](#_Toc444528072)

[1.5.5 Disclaimers 12](#_Toc444528073)

[1.6 Violations and Reporting 12](#_Toc444528074)

[Staff undertaking 13](#_Toc444528075)

# Staff policies on data security and confidentiality

## Introduction.

This document sets out the procedures for observing confidentiality and security of data within the Registry. 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 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 by health care professionals in particular, to observe the highest standards of security and confidentiality with regard to the very sensitive information which we have in our possession. Those of us handling this information every day may sometimes forget the potential consequences its disclosure might have for individuals or their families. We must also be aware of the disastrous consequences for the Registry, 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 (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 (GMS number, PPS number, hospital medical record number), or indirectly through a unique combination of personal characteristics.

Apart from confidential personal information, the Registry 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.

Registry 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 accidentally. Staff must not abuse their privileges of access to medical records by seeking information not relevant to their work.

## Data security

### 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 "Guidelines for staff on confidentiality within the National Cancer Registry".
* sign an undertaking of confidentiality, which will remain binding even following their departure from Registry work. This undertaking prohibits staff from disclosing, either directly or indirectly, to any individual outside the Registry or to other staff within the Registry 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 Registry.

### Physical security

The operation of the Registry is largely electronic, and few written documents containing individual identification are created. Any such written documents are to be shredded immediately after use. Documents which need to be kept for archival purposes are to be stored securely in areas specifically designated for this purpose and in locked storage cabinets. Access to these cabinets is limited to authorised Registry personnel.

The Registry door is to be kept locked at all times. Visitors to the Registry must be admitted to the Registry 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 could be visible. Unless there is a specific reason for doing otherwise, visitors should be confined to the non-secure areas of the Registry (meeting rooms, lobby, Director’s office).

The Registry premises are protected by high-security locks and by electronic alarms. Non-Registry 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.

### Electronic security

Data collected by Registry staff on laptop computers is password protected and encoded, and must also be encoded during any transmission to and from the Registry. Data is stored on laptop computers in a 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 Registry and all staff are required to comply with the laptop security policy. Details of the Registry’s security policy specific to laptops are outlined in section 5.3 page 23). Staff should adhere strictly to the laptop security policy (Section 5.3) If any breach of security is suspected, the Director should be informed immediately. Password policies with regard to laptop password format and frequency of change must be complied with.

Data within the Registry is protected by passwords and encoding. Each individual within the Registry has a personal password, which defines their level of access to the computer system. Password policies with regard to password format and frequency of change must be complied with. Passwords must never be written down anywhere and must be encrypted if stored in electronic format. A second password is needed for access to the patient database. 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 Registry, and not to allow any identifiable data to appear on the screen while leaving their desk. Registry computers which contain personally identifiable data are not 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 all valuable data is backed up regularly. Data held locally should be backed up to the network at least weekly. No confidential data should be held on local PCs.

#### 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.

#### It is the responsibility of the IT department to assign unique passwords to all staff – the users will be given their passwords directly by a member of IT – the passwords will include:

#### Power on passwords (Safend password or TrueCrypt password)

#### Log on to Windows password (on laptops with a Windows 2000/XP/2007 Operating System)

#### National Cancer Registry System password

#### Once you have memorised your password any written notes should be shredded

#### Do not reveal your passwords to anyone

#### Do not write down your passwords

#### If you suspect your password has been compromised please notify the IT department immediately

#### If the password is lost the IT department will set a new one

#### Safend Encryptor/TrueCrypt Software

Safend Encryptor/TrueCrypt software provides a solution for protecting confidential data; it encrypts the data stored on laptops and the result is that confidential data cannot be read by any unauthorised user in the case of loss or theft. This software is installed on all Registry laptops.

#### 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.  Examples include, but are not limited to, USB keys, CDs, Flash drives, DVDs and diskettes.

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 Registry data or data pertaining to the Registry or cancer registration.

* Only devices issued or approved by the IT department should be used.
* It is essential that a removable media device is encrypted to an accepted 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 Registry or gives an indication of the nature of the data contained on it.
* 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.
* When a removable media device is removed from the office, the user should be aware of the 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, the data should be transferred to a PC, laptop or server as soon as possible.  This transfer should include the removal of the data from the removable media device.
* Where a removable media device is used to transfer data from one machine or device to another, the data should be removed from the device at the end of the process.

#### PGP Software

Each member of the Research Team in the Registry has PGP installed. By default, as a minimum, they will always encrypt to their own key and this “master” key so that in case of emergency (something happening to them so we can’t use their private key and pass-phrase) the Director will be able to decrypt the files.

The copy of the private and public keys for this PGP “master” key (you need the private key, along with the pass-phrase that only the Director knows, to decrypt files) are in the folder [\\Gauguin\IT\Infrastructure\Security](file:///%5C%5CGauguin%5CIT%5CInfrastructure%5CSecurity).

#### Filesender

An alternative to PGP Software is FileSender from HEANet. 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.

#### 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.

The NCRI have signed up the 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.

#### Virus Protection

##### Things to do to protect yourself:

Ensure that you have activated anti-virus software on your PC/laptop and that it is configured for automatic update. Always scan software disks and files with approved anti-virus software. . It is imperative that the anti-virus software is not disabled on your PC/laptop. If you suspect there is any issue with your anti-virus software, please notify IT immediately.

##### What to do if you suspect a virus:

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

### Security during data collection and processing

1. The arrangements for security and confidentiality within each hospital must be strictly observed. Medical records should not be taken from areas assigned to them without the specific permission of a responsible hospital authority.
2. All confidential material must be stored out of sight when not personally attended.
3. 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.
4. Material that is not pertinent to Registry work should never be examined.
5. 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.
6. 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.
7. All printed records, questionnaires and interviews records with personal data should be shredded as soon as they are no longer needed.
8. When printing reports for internal use, avoid the use of identifiers, unless this is essential for the purpose of the report.

### Communication

#### Email

1. The email system is intended for the business purposes of the Registry. The email account is not intended for personal use (see Internet and email policy) but limited personal use is acceptable. However, the Registry reserves the right to curtail or prohibit all, or specific, personal usage.
2. When forwarding emails it is important to check for sensitive, inappropriate or confidential information in the message being forwarded.
3. Standard unencrypted email should never be used to transmit confidential data. Please see [1.2.3.6](#_Healthmail) [Healthmail](#_Healthmail) for information on sending confidential data via e-mail.

#### Telephone

1. Information concerning identifiable patients or research subjects should **never** be given over the telephone to non-Registry staff.
2. 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).
3. If there is any possibility that confidential information might be overheard in the general office, use the designated soundproof rooms.
4. Staff using offices shared with non-Registry staff should not discuss confidential information if the office is occupied.
5. 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
	1. Asking that the person write in for information which can be sent directly, or to a named medical practitioner
	2. Asking permission to telephone the person’s GP with the information.

On occasion, family members of patients may contact the Registry, 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.

#### Letters

1. 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.
2. Any communication between Registry staff with regard to patients should use patients' registration numbers, not names and/or addresses. Material should be sent electronically and encrypted, rather than by post, if possible.

#### Fax Machines

The use of fax machines to transmit identifiable data should be avoided. However, it may sometimes be necessary to fax material, for instance TROs may need to forward a list of cases to a hospital medical records department; research questionnaires may need to be faxed. In this case, the following procedure must be observed:

1. Send only the information required.
2. The list should be faxed to a designated person who is aware that it is coming and of its content.
3. This person should be available to receive the fax and should have adequate security measures in place e.g. the fax should not be left unattended in an open plan office.
4. Double check the fax number before dialling.
5. Ring or email the designated person and confirm that they have received the fax.
6. Use a cover sheet with recipient’s name clearly entered, this will let anyone know who the information is for and whether it is confidential or sensitive without having to look at the contents.
7. The document faxed, and that received, must be shredded after use.

## Laptop Security Policy

**The same general provisions apply to laptop use as to computer use at the main Registry offices (see sections 5.2.3 to 5.2.7). The principles below are more specific to off-site use .**

### Purpose

This policy addresses the actions that must be taken by all Registry staff who have a Registry laptop, or who are temporarily using a “shared” Registry laptop, or the laptop of another employee.

### Requirements

All laptops acquired for, or on behalf of, the Registry 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 Registry policy on storage and transport of your laptop, your line manager and the IT department must be informed and alternative arrangements approved.**

### Storage and transport outside the main Registry offices

* 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.
* Kensington locks must be used by tumour registration officers and IPCOR researchers when storing the laptop outside their base office.
* 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.
* The laptop must never be left unattended in a parked car.
* 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 Registry offices or (for tumour registration officers) in the base office. If you are unable to do this the IT Administrator must be notified.
* Unaccompanied shipment of laptops to and from the Registry must be arranged by, or with the approval of, the IT department, using an approved courier.

### Laptop usage outside Registry offices

* Confidential data should never be held on a laptop without the use of Registry installed encryption software.
* Laptops should be used **only** for Registry work.
* Software should be installed only by Registry IT staff.
* 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 by using the Ctrl+Alt+Delete command as well as attaching the Kensington lock supplied by the Registry. If you are unable to use the Kensington lock the IT Administrator must be notified of this and a log of risk hospitals will be maintained by the IT Administrator.

If you need to leave the office disconnect from the Registry’s network and from the internet. If using a “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 tumour registration officers or IPCOR researchers use a laptop to connect to the Registry server in Cork, they should connect only to systems they are authorised to use. Tumour registration officers and IPCOR researchers should always log off the Registry server during periods of inactivity.

### Violation and Penalties

* Employees should comply with this policy as far as reasonably possible.
* Violation of this policy may be grounds for disciplinary action.

### 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.

#### 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.

#### 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.

#### 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.

## Breaches of data security or confidentiality

### Loss or disclosure of confidential data

#### 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, the Director should be contacted. The Director will nominate someone to be responsible for data security in his absence
2. This 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.
3. 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.
4. If data has been lost or mislaid and it can possibly be retrieved before it is read by anyone outside the Registry 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.
5. 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.

#### Procedures for the responsible person

1. If confidential data has been disclosed to unauthorized persons the Data Protection Commissioner must be informed.
2. All breaches of confidentiality, or suspected breaches, must be reported to the Director, or in his absence a nominated responsible person, as soon as possible.
3. Risk assessment should be carried out—what type of data is involved, has it been lost or disclosed, to whom, is this Registry or third party (e.g. pathology report) information?
4. Has there been a breach of procedure? If so, is there a possibility of disciplinary action?

### 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 y the IT Manager.
3. The Director, or in his 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.

## Internet, Network and Email Policy

### Introduction

The National Cancer Registry aims to provide you with accessible, up-to-date and reliable information to support you in your work. This goal requires the Registry 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 Registry. 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 Registry activities. Users must not attempt to bypass any of the Registry’s security features. The Registry reserves the right to block unacceptable content that may be dangerous to the network

### General Internet Use

#### User accountability

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

#### Virus Detection

All files obtained from sources outside the organisation, or downloaded over the Internet should not be opened without first scanning the material with Registry approved virus checking software which is presently McAfee. If you suspect that a virus has been introduced into the Registry network, notify the IT group immediately.

#### 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.

#### 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 Registry.
* Using software that transmits and receives content over a network which has not been expressly approved by the Registry. A list of acceptable software is available from the IT Administrator.
* Storing works containing unacceptable or illegal content either locally or on any other machine on a network administered by the Registry.

#### 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.

### Email

This sets forth the policy of Registry with respect to email & internet usage. All individuals (including but not limited to staff, outside consultants and visitors) who use the Registry 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.

#### General Principles

##### Acceptable use

* The email system is meant to be used for the business purposes of the Registry. Limited personal use is acceptable provided it complies with Registry policy on content. However, the Registry reserves the right to curtail or prohibit all, or specific, personal usage.
* Standard unencrypted email should **never** be used to transmit any confidential data (i.e. personal or sensitive data).
* When sending emails concerning registered or potential patients or research subjects, the following precautions must be observed:
	+ If un-encrypted, all identifiable details (including hospital name) must be removed before sending the email. The email should contain the registration number only, if an identifier is needed.
	+ Ensure that the email is only sent to the intended recipient. Double-check before sending.
	+ Check that the recipient has received the email; if they have not, inform the IT department and your line manager immediately
	+ If you are unsure if the email should be encrypted or password protected, contact your line manager or the IT department for clarification.

##### Ownership

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

#### Email Review

All email is subject to the right of the Registry 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 Registry for any violations of law, breaches of Registry policies, communications harmful to the Registry, or for any other reason. Registry also reserves the right to disclose emails to authorised persons.

#### Email Content

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

#### Security

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

### 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 DP 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 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.

#### 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.

#### 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.

#### 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.

#### 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.

#### 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.

#### 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.

#### 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.

### Disclaimers

A disclaimer is appended to all outgoing messages from a Registry e-mail account, where the recipient is external to the Registry. When using registry webmail (but not other webmail such as Gmail, Hotmail) the user must append the following disclaimer themselves.

 *The contents of this email are intended for the named addressee only. It contains information that may be confidential. Unless you are the named addressee or an authorised designee, you may not copy or use it, or disclose it to anyone else. If you have received it in error please notify us immediately and then destroy it. The Registry does not guarantee the security of any information electronically transmitted and is not liable if the information contained in this communication is not a proper and complete record of the message as transmitted by the sender or for any delay in its receipt.*

In Outlook web-interface you can save this as a *signature* which you can choose to append to your messages. This saves you the effort of typing it in every time. A representative of the IT Group will configure this for you if you wish.

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.

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

**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: