RCSI

Data Protection in

Royal College of Surgeons in Ireland

September 2015

CONTENTS

1. RCSI POLICIES AND PROCEDURES

1.1 Data Protection Policy Statement

1.2 Data Access Procedure

1.3 Data Breach Procedure

1. RCSI POLICIES AND PROCEDURES

Purpose

Data Protection is an increasingly important issue for all organisations, as public awareness of privacy rights is increasing alongside rapid technological changes and constantly evolving methods of collecting, storing and sharing personal data.

Like all organisations that hold and use personal data, the Royal College of Surgeons in Ireland must meet certain obligations relating to the manner in which it collects, stores, uses and disseminates personal data of individuals.

This portfolio draws together a number of documents which are of direct relevance to RCSI's ability to meet these various obligations. These policies and procedures have been drafted in order to address the college's general obligations in the area of data protection and to ensure staff are aware of their responsibilities in the event of access requests and data breaches occurring.

The following pages set out:

- RCSI's Data Protection Policy
- Procedures on Subject Access Requests and Data Breach Management

1.1 DATA PROTECTION POLICY STATEMENT

Background

The Royal College of Surgeons in Ireland (RCSI) is committed to meeting its obligations under the Data Protection Acts 1988 and 2003 ('the Acts').

RCSI needs to collect personal data, as defined by the Acts, for a variety of purposes, in order to conduct its business as a health sciences institution. RCSI collects data relating to staff, students, researchers and other individuals who come into contact with the college in the course of its activities.

Personal data is collected, managed and used for a variety of purposes including, but not limited to, the admission, assessment and examination of students and their academic performance, the management and conduct of research activities, the recruitment and payment of staff.

Purpose

The purpose of this policy is to clearly state the commitment of RCSI to meeting its obligations under the Acts and to briefly describe the structures and procedures that are in place in order to ensure compliance.

Scope

This policy applies to:

- any person who is employed by RCSI or is engaged by RCSI and who processes personal data in the course of their employment or engagement for administrative, research and/or any other purpose;
- individuals who are not directly employed by RCSI, but who are employed by contractors (or subcontractors) and who process personal data in the course of their duties for RCSI;
- individuals who are not directly employed by RCSI but who are employed by external companies, agencies, institutions, pubic bodies or organisations and who have, or potentially have access to personal data as part of their interaction with RCSI
- RCSI clubs and societies.

What types of data does this policy apply to?

This policy applies to:

- all personal data created or received by the College in any format (including paper records), whether used in the workplace, stored on portable devices and media, transported from the workplace physically or electronically or accessed remotely;
- personal data held on all College IT systems managed centrally by the IT Department, and locally by individual Colleges/Schools/Departments/Offices/Institutes or Centres;
- any other IT systems on which College data is held or processed
- any set of hard copy records generated or received by the College or associated agencies containing personal data, whether stored on RCSI premises or at other locations

This policy is to be implemented in conjunction with other relevant RCSI policies, including the *Records Management Policy, IT Acceptable Usage Policy, Encryption Policy, Conditions of Use of IT Systems and Resources* and any other relevant policies that may be introduced by College authorities.

Failure to comply with this policy may lead to disciplinary action, up to and including dismissal in the case of staff, being taken in accordance with RCSI's disciplinary procedures. Failure of a third party contractor/subcontractor to comply with this policy may lead to termination of the contract and/or legal action.

Principles

RCSI commits itself to compliance with the eight principles of data protection as set out in the Acts, i.e.

1. **To obtain and process personal data fairly**

   RCSI will obtain and process personal data fairly in accordance its legal obligations.

2. **To keep it only for one or more specified and lawful purposes**

   RCSI will keep data for purposes that are specific, lawful and clearly stated and the data will only be processed in a manner compatible with these purposes.

3. **To use and disclose it only in ways compatible with the stated purpose(s)**

   RCSI will only use and disclose personal data in ways that are necessary for the purpose/s or compatible with the purpose/s for which it collects and keeps the data.

4. **To keep it safe and secure**

   RCSI will take appropriate technical and organisational security measures against unauthorised access to, or alteration, disclosure or destruction of the data and against their accidental loss or destruction.

5. **To keep it accurate, complete and up-to-date**

   RCSI will take appropriate measures to ensure high levels of data accuracy and completeness and to ensure that personal data is kept up to date.

6. **To ensure that it is adequate, relevant and not excessive**

   Personal data held by the College will be adequate, relevant and not excessive in relation to the purpose/s for which they are kept.

7. **To retain it for no longer than is necessary for the purpose for which it was collected**

   RCSI will have a defined retention period policy for personal data and appropriate procedures in place to implement such a policy.

8. **To give a copy of his/her personal data to an individual, upon request.**

   RCSI will have procedures in place to ensure that data subjects can access a copy of his/her data held by RCSI, in compliance with sections 3 & 4 of the Data Protection Acts.

Structures/Roles

Overall responsibility for compliance with Data Protection principles and the Acts lies with Council as the overall governing body of RCSI and with the Senior Management Team.

The RCSI Records and Information Compliance Manager (RICM) is the nominated Data Protection Officer for RCSI with overall responsibility for Data Protection policy and procedures, including staff training and awareness and providing advice in responding to all data protection queries. The RICM may convene working groups or committees as appropriate in order to facilitate awareness and compliance.

Responsibility for technical protection and security of personal data rests with RCSI's Information Technology Department.

The Head of Department is responsible for ensuring that his/her Department or Office has appropriate procedures in place to ensure compliance with this policy. A Head of Department may delegate responsibility to an appropriate member of staff within his/her Office or Department.

All employees of RCSI who process personal data are also individually responsible for compliance with data protection, in accordance with the Acts.

Review

This policy will be reviewed annually in order to ensure ongoing relevance and effectiveness. More frequent reviews may take place in certain circumstances, for example in response to new legislation or regulations.

Professor Cathal Kelly, CEO/Registrar

September 2015

1.2 DATA ACCESS PROCEDURE

Introduction

This document outlines the procedure to be followed by individuals who wish to access personal data about themselves which is held by the Royal College of Surgeons in Ireland.

Procedure

If an individual wishes to make a data access request, it must be in writing.

Please complete and sign the application form (Appendix 1) and send it by post or email to RCSI's Records and Information Compliance Manager (RICM) (contact details below).

If a third party wishes to allow a third party submit a data access request on their behalf (e.g. a family member or solicitor), the individual must provide written authorisation to allow RCSI to disclose their personal data to that third party (see Section 7, Appendix 1).

Fee

Please note that a fee of €6.35 must accompany your data access request (cheque or postal order to be made payable to Royal college of Surgeons in Ireland. Please do not send cash by post.

We will not begin to search for your personal data until the application fee is paid.

Identification

In order to ensure that personal data is not disclosed to the wrong person, you must provide proof of identity with your data access request i.e. a photo ID and confirmation of your current address.

Acceptable forms of identification include: copy of passport or driving licence; staff ID card; copy of utility bill.

Copies are acceptable in most cases; however we reserve the right to ask to see original documents where necessary. Copies of such documents sent with your data access request will be securely destroyed once we have verified your identity.

Where to send your request

All requests for access to personal data held by RCSI should be sent to:

Records & Information Compliance Manager

Address: Royal College of Surgeons, Mercer Library, Mercer Street, Dublin 2.

Telephone: 01 4022425

Email: data.protection@rcsi.ie

A decision on your request will be made within 40 days of receipt of your request, application fee and identification.

Right to complain to Data Protection Commissioner

If you are unhappy with the outcome of your request, you may make a complaint to the Data Protection Commissioner (Canal House, Station Road, Portarlington, Co. Laois), who will investigate the matter for you. Further details on your rights under the Data Protection Acts are available on the Data Protection Commissioner's website www.dataprotection.ie

Review

These procedures will be reviewed annually by RCSI's RICM and they may be reviewed or amended from time to time.

Appendix 1

Data Access Request Form

SECTION 1 – YOUR DETAILS (PLEASE USE BLOCK CAPITALS)

Surname:	
First Name(s):	
Previously known as (if applicable):	
Address:	
Date of birth:	
Telephone number:	
Email address:	

SECTION 2 – YOUR RELATIONSHIP WITH RCSI

Are you a current/former* member of staff?	YES / NO* *(*delete as appropriate)*
If yes, please provide the following details:	
Staff Number:	
Department/Office:	
If you are not a member of staff, please indicate your relationship with the College, including dates:	

The information in sections 1 and 2 will be used to enable staff of RCSI to correctly identify any personal data relating to you and to cross-check your identity before records (should any exist) are released.

SECTION 3 – PERSONAL DATA REQUESTED

In the box below, please provide as much detail as you can about the personal data you wish to access in order to help us locate it quickly.

In accordance with the Data Protection Acts, 1988 and 2003, I request access to the following personal data that I believe RCSI holds about me:

SECTION 4 – FEES

A fee of €6.35 must accompany this data access request form. **Cheques should be made payable to Royal College of Surgeons in Ireland. Please do not send cash by post.**

SECTION 5 – IDENTIFICATION

In order for us to protect the security of personal data, it is necessary for you to provide proof of your identity by providing a photo ID and proof of your current address. Acceptable forms of identification include: Copy of passport or driving licence Staff/student ID Card Copy of utility bill

Please complete *either* section 6 *or* section 7 as appropriate

SECTION 6 – DECLARATION OF DATA SUBJECT

I confirm that I am the data subject named in Section 1 and I am requesting access to my own personal data. I understand that the information I have supplied will be used to administer my access request, to confirm my identity and to help locate the information I have requested. I also understand that it may be used for statistical purposes.	
Signed:	Date:

SECTION 7 – DECLARATION OF DATA SUBJECT FOR AGENT TO ACT ON THEIR BEHALF

If you wish someone else to submit a data access on your behalf (e.g. family member, solicitor) please complete this section.

I confirm that I am the data subject named in Section 1. I give permission for the person or organisation named below to act on my behalf in relation to my data access request. I have enclosed proof of my identity referred to in Section 5 and confirm that I wish my personal data to be sent to my representative at the address below. I understand that the information I have supplied will be used to confirm my identity and help locate the information I have requested. I also understand that it may be used for statistical purposes.	
Signed:	Date:

Name of agent:	
Relationship to data subject:	
Address:	

Telephone number:	
Email address:	

Please note: any agent other than a professional advisor (e.g. solicitor) nominated by you must provide two forms of ID as per Section 5 above in order to verify his/her identity.

PLEASE RETURN THE COMPLETED FORM TO:

data.protection@rcsi.ie

or by post to:

Records & Information Compliance Manager,

Royal College of Surgeons, Mercer Library, Mercer Street, Dublin 2.

.

1.3 DATA BREACH POLICY

Introduction

The Royal College of Surgeons in Ireland ("the College") is obliged under the Data Protection Acts, 1988 and 2003 ('the Acts), to keep personal data safe and secure and to respond promptly and appropriately to data security breaches. The College's commitment to meeting its obligations in this regard is set out in the Data Protection Policy Statement.

Purpose

The purpose of these procedures is to provide a framework for reporting and managing data security breaches affecting personal or sensitive personal data held by the College.

It is vital to take prompt action in the event of any actual, potential or suspected breaches of data security or confidentiality, in order to avoid the risk of harm to individuals and legal, financial and reputational costs to the College.

What is a Personal Data Security Breach?

A personal data security breach is any event that has the potential to affect the confidentiality, integrity or availability of personal data held by the College in any format.

A breach can include but is not limited to:

- the disclosure of confidential data to unauthorised individuals;
- loss or theft of data or equipment on which data is stored;
- loss or theft of paper records;
- inappropriate access controls allowing unauthorised use of information;
- suspected breach of the College's IT security policies;
- attempts to gain unauthorised access to computer systems, e.g. hacking;
- viruses or other security attacks on IT equipment systems or networks;
- breaches of physical security e.g. forcing of doors or windows into secure rooms or filing cabinets containing confidential information;
- confidential information left unlocked in accessible areas;
- leaving IT equipment unattended when logged-in to a user account without locking the screen to stop others accessing information;
- emails containing personal or sensitive information sent in error to the wrong recipient.

Who is responsible for managing personal data security breaches?

Personal data security breaches are managed by the RICM in conjunction with the relevant RCSI Heads of Department, staff and managers and, where appropriate, the Academic Council and Senior Management Team.

Procedure for reporting personal data security breaches

In the event of a breach of personal data security occurring, it is vital to ensure that it is dealt with immediately and appropriately to minimise the impact of the breach and to prevent a recurrence.

Any person acting on behalf of RCSI who becomes aware of an actual, potential or suspected breach of personal data security, must report the incident to their line manager immediately.

The relevant manager must then:

Report the incident immediately to the RICM (and to the Head of the relevant Department/School/Unit etc, if desired)

- During office hours: e-mail data.protection@rcsi.ie or phone ext 2425
- Outside of Office Hours, phone (087) 2381016

Complete the attached Data Security Breach Report Form and email it to the RICM as soon as possible.

This will enable all the relevant details of the incident to be recorded consistently and communicated on a need-to-know basis to relevant staff so that prompt and appropriate action can be taken to resolve the incident.

Procedure for managing data security breaches

In line with best practice[1], the following five steps should be followed in responding to a data security breach:

Step 1: Identification and initial assessment

Step 2: Containment and recovery

Step 3: Risk assessment

Step 4: Notification

Step 5: Evaluation and response

Step1: Identification and initial assessment of the incident

If an agent of the College considers that a data security breach has occurred, this must be reported immediately to the relevant line manager/Head of Department who will in turn notify the RICM (phone 01-4022425 or email data.protection@rcsi.ie), outlining briefly the nature of the suspected breach.

The line manager/Head of Department should complete part 1 of the Data Security Breach Report Form and return it to the RICM without delay. Part 1 of the Report Form will assist the RICM in conducting an initial assessment of the incident by establishing:

- if a personal data security breach has taken place;
- what personal data is involved in the breach;
- the cause of the breach;
- the extent of the breach (how many individuals are affected/may potentially be affected);
- the harm to affected individuals that could potentially be caused by the breach (e.g. financial, private lives etc.);
- how the breach can be contained.

Following this initial assessment of the incident, the RICM will initiate an investigation of the incident. The RICM may nominate another officer of the College for this purpose, or may, if it is deemed necessary, nominate a group of relevant College stakeholders to assist with the investigation. Any records relating directly to an investigation will be retained by the RICM.

The RICM (or other nominated officer/s) will determine the severity of the incident using the checklist in Appendix 2 and by completing part 2 of the Data Security Breach Report Form (i.e. s/he will decide if the incident can be managed and controlled locally or if it is necessary to escalate the

[1] Office of the Data Protection Commissioner, '*Personal Data Security Breach Code of Practice*'

incident to the Senior Management Team). The severity of the incident will be categorised as level 1, 2 or 3 as follows:

Level 1 incident requiring no further action or reporting, beyond those directly involved.

Level 2 incident requiring internal investigation and action involving management and senior staff in selected areas.

Level 3 incident requiring action by SMT, external reporting and the possible involvement of external agencies such as the Office of the Data Protection Commissioner and/or the Gardaí.

Step 2: Containment and Recovery

Once it has been established that a data breach has occurred, the College needs to take immediate and appropriate action to limit the breach.

The RICM, liaising with relevant College staff members/managers, will:

Establish who within the College needs to be made aware of the breach (e.g. IT Department, Estate & Support Services, SARA, Dean's Office, School of Postgraduate Studies, Legal Affairs, Communications Department, etc.) and inform them of what they are expected to do to contain the breach (e.g. isolating/closing a compromised section of the network, finding a lost piece of equipment, changing access arrangements to file storage areas, etc.)

Establish whether there is anything that can be done to recover any losses and limit the damage the breach can cause (e.g. physical recovery of equipment/records, the use of back-up tapes to restore lost/damaged data).

Establish if it is appropriate to notify affected individuals immediately (e.g. where there is a high level of risk of harm or damage to individuals).

Where appropriate (e.g. in cases involving theft or other criminal activity), inform the Gardaí or the Office of the Data Protection Commissioner.

Step 3: Risk Assessment

In assessing the risk arising from a data security breach, the relevant College stakeholders are required to consider the potential adverse consequences for the individual. The information provided at Stage 1 on the Data Security Breach Report Form will assist with this stage.

The RICM (or nominated officer/s) in conjunction with the Head of Department/unit/institute/centre in which the incident occurred will review the incident report to:

Assess the risks and consequences of the breach:

- Risks for individuals:
    - What are the potential adverse consequences for individuals?

    - How serious or substantial are these consequences?
    - How likely are they to happen?
- Risks for the College:
    - Strategic & Operational
    - Compliance/Legal
    - Financial
    - Reputational
    - Continuity of Service Levels

Determine, where appropriate, what further remedial action should be taken on the basis of the incident report in order to mitigate the impact of the breach and prevent repetition.

The RICM (or nominated officer/s) will prepare a report setting out (where applicable):

- a summary of the security breach;
- the people involved in the security breach, (such as staff members, students, contractors, external clients);
- details of the information, IT systems, equipment or devices involved in the security breach and any information lost or compromised as a result of the incident;
- how the breach occurred;
- actions taken to resolve the breach;
- impact of the security breach;
- unrealised, potential consequences of the security breach;
- possible courses of action to prevent a repetition of the security breach;
- side effects, if any, of those courses of action;
- recommendations for future actions and improvements in data protection as relevant to the incident.

The incident report will then be furnished to relevant parties as follows:

Level 1 incidents: to the staff and managers directly involved in the process which led to the breach. Line Managers have the option to share the incident report with Head of Department/School/Unit/Institute or Centre (as appropriate).

Level 2 incident: to the Head of School/Department/Unit/Institute or Centre where the breach occurred and to their counterparts in other units affected, or which may be affected by similar issues in future.

Level 3 incident: to the Chief Executive Officer and Senior Management Team, as well as the relevant Head of School/Department/Unit/Institute and other staff and management as appropriate

Step 4: Notification

On the basis of the evaluation of risks and consequences, the RICM, and others involved in the incident as appropriate, will determine whether it is necessary to notify the breach to others outside the College.

For example:

- individuals (data subjects) affected by the breach;
- the Data Protection Commissioner;
- other bodies such as regulatory bodies, grant funders;
- external legal advisers
- the press/media;
- the College's insurers
- bank or credit card companies
- the Gardaí;
- trade unions

As well as deciding **who** to notify, the College must consider:

What is the message that needs to be put across?

In each case, the notification should include as a minimum:

- a description of how and when the breach occurred;
- what data was involved;
- what action has been taken to respond to the risks posed by the breach.

When notifying individuals, the College should give specific and clear advice on what steps they can take to protect themselves, what the College is willing to do to assist them and details of how they can contact the College for further information (e.g. helpline, website).

In accordance with the Data Protection Commissioner's ***Personal Data Security Breach Code of Practice***[2], all incidents in which personal data has been put at risk should be reported to the Office of the Data Protection Commissioner (ODPC) as soon as the College becomes aware of the incident, except when:

- the full extent and consequences of the incident has been reported without delay directly to the affected data subject(s) **and**
- it affects no more than 100 data subjects **and**
- it does not include sensitive personal data or personal data of a financial nature.

In case of doubt – in particular any doubt related to the adequacy of technological risk-mitigation measures – the College should report the incident to the ODPC.

Any contact with the Data Protection Commissioner should be made through the RICM. Initial contact with the OPDC should be made by the RICM within two working days of becoming aware of the breach, outlining the circumstances surrounding the incident.

The ODPC will make a determination regarding the need for a detailed report and/or subsequent investigation based on the nature of the incident and the presence or otherwise of appropriate physical or technological security measures to protect the data.

In cases where the decision is made by the RICM not to report a breach, a brief summary of the incident with an explanation of the basis for not informing the Data Protection Commissioner will be retained by the RICM.

NOTE: It is advisable that the Communications Department is informed prior to any notification being made.

Step 5: Evaluation & Response

Subsequent to a data security breach, a review of the incident by the RICM in consultation with the relevant stakeholders in the College will take place to ensure that the steps taken during the incident were appropriate and to identify areas that may need to be improved.

The RICM will retain all data security breach reports and will use them to compile a central record of incidents. The RICM will report on incidents to the Senior Management team on an annual basis in order to identify lessons to be learned, patterns of incidents and evidence of weakness and exposures that need to be addressed.

---

[2] http://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm

For each Level 3 incident, the RICM will conduct a review to consider and report to the Senior Management Team on the following:

- What action needs to be taken to reduce the risk of future breaches and minimise their impact?
- Whether policies, procedures or reporting lines need to be improved to increase the effectiveness of the response to the breach?
- Are there weak points in security controls that need to be strengthened?
- Are staff and users of services aware of their responsibilities for information security and adequately trained?
- Is additional investment required to reduce exposure and if so what are the resource implications?

Related Policies and Procedures

These procedures are complementary to and should be read in conjunction with other College policies and procedures, including:

- Data Protection Policy (link to be inserted)
- Acceptable Usage Policy
- Encryption Policy
- Conditions of Use of IT Systems and Resources
- E-mail Policy
- Internet Policy
- Records Management Policy
- Research Ethics and Integrity Requirements

RCSI staff should ensure compliance with the above policies and procedures in addition to these Data Breach Management Procedures.

Further Help and Advice

For further information and advice about this procedure and about data protection matters, please contact:

Records & Information Compliance Manager

data.protection@rcsi.ie

RCSI Mercer Library, Mercer Street, Dublin 2

01-4022425

APPENDIX 1 – PERSONAL DATA SECURITY BREACH REPORT FORM

Please act promptly to report any data security breaches. If you discover a data security breach, please notify your line manager immediately. Heads of Department/Office to complete Section 1 of this form and email it to the RICM at data.protection@rcsi.ie

Section 1: Notification of Data Security Breach	**To be completed by person reporting incident**
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number, RCSI address):	
Brief description of incident or details of the information lost:	
Number of Data Subjects affected, if known:	
Has any personal data been placed at risk? If, so please provide details	
Brief description of any action taken at the time of discovery:	

For College use	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	

Section 2: Assessment of Severity	To be completed by RICM in consultation with relevant staff of area affected by the breach
Details of the IT systems, equipment, devices, records involved in the security breach:	
Details of information loss:	
What is the nature of the information lost?	
How much data has been lost? If laptop lost/stolen: how recently was the laptop backed up onto central IT systems?	
Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for the College or third parties?	
How many data subjects are affected?	
Is the data bound by any contractual security arrangements e.g. to research sponsors?	
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories:	
<u>HIGH RISK</u> personal data **Sensitive personal data (as defined in the Data Protection Acts) relating to a living, identifiable individual's** **racial or ethnic origin;** **political opinions or religious or philosophical beliefs;** **membership of a trade union;** **physical or mental health or condition or sexual life;** **commission or alleged commission of any**	

offence, or **proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.**	
Information that could be used to commit identity fraud such as personal bank account and other financial information and national identifiers, such as Personal Public Service Numbers (PPSNs) and copies of passports and visas;	
Personal information relating to vulnerable adults and children;	
Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed;	
Spreadsheets of marks or grades obtained by students, information about individual cases of student discipline or sensitive negotiations which could adversely affect individuals.	
Security information that would compromise the safety of individuals if disclosed.	
Category of incident (1, 2, or 3):	
Reported to RICM on:	
If level 2 or level 3, date escalated to Head of Department and/or Senior Management Team	

Section 3: Action taken	To be completed by RICM
Incident number	
Report received by:	
Date received:	
Action taken by responsible officer/s :	
Was incident reported to Office of Data Protection Commissioner?	**Yes/No** **If YES, notified on (date):**
If NO, reason for non-reporting	
Follow up action required/recommended:	
Was incident reported to the data subjects affected?	**Yes/No**
If YES, date on which reported and method used (letter, e-mail, etc.):	
If NO, reason for non-reporting:	
Reported to other internal or external stakeholders?	**Yes/No**
If YES, details of agencies informed, and dates:	

APPENDIX 2 – CHECKLIST FOR ASSESSING SEVERITY OF THE INCIDENT

How serious is the incident?

Level 1 Incident:

A Level 1 Incident features limited disruption to services (department, building or College); no serious threat to life, property or the environment; no threat to RCSI's image/reputation.

Can the consequences of the security breach, loss or unavailability of the asset be managed locally within normal operating procedures?

If so, manage the incident according to the Data Security Breach Management Procedure (this procedure).

Level 2 Incident

A Level 2 Incident features disruption to the functioning capacity of a key College building or a key service. Such a situation or incident (actual or potential) may pose a threat to privacy for a restricted number of people and does not involve sensitive personal data.

In addressing this incident, is assistance required from other members of staff within the College or specialist support teams outside the College?

Does the breach warrant reporting to the relevant Head of Department and/or other senior managers?

If so, the RICM, in conjunction with other staff involved in dealing with the incident, will decide who else needs to assist or be made aware of the breach.

Level 3 Incident

Does the loss or breach of data security involve high risk personal data, i.e.:

- **Sensitive personal data** (as defined in the Data Protection Acts) relating to a living, identifiable individual's
  - racial or ethnic origin;
  - political opinions or religious or philosophical beliefs;
  - membership of a trade union;
  - physical or mental health or condition or sexual life;
  - commission or alleged commission of any offence, or

- proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.
- Information that could be used to commit identity fraud such as personal bank account and other financial information and national identifiers, such as Personal Public Service Numbers (PPSNs) and copies of passports and visas;

- Personal information relating to vulnerable adults and children;
- Detailed profiles of individuals; including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed;
- Spreadsheets of marks or grades obtained by students, information about individual cases of student discipline or sensitive negotiations which could adversely affect individuals.
- Security information that would compromise the safety of individuals if disclosed.
- Are more than 100 individuals affected by the incident?
- Is the information involved of such a nature that the breach should be reported to the Gardai or other external agencies?

If so, then the RICM, in conjunction with relevant staff, should report the incident to the Senior Management Team and make contact with relevant external agencies and data subjects.

*****