



**THE COUNCIL OF LEGAL EDUCATION  
THE NORMAN MANLEY LAW SCHOOL**

**PERSONAL DATA INCIDENT RESPONSE POLICY**

## Table of Contents

<b>DEFINITIONS:</b> .....	ii
<b>1.0 TITLE: Personal Data Incident Response Policy</b> .....	1
<b>2.0 POLICY STATEMENT</b> .....	1
<b>3.0 PURPOSE</b> .....	1
<b>4.0 SCOPE</b> .....	2
<b>5.0 PROCEDURE</b> .....	3
<b>6.0 RESPONSIBILITIES</b> .....	4
<b>6.1 Compliance/Monitoring/Review</b> .....	4
<b>6.1.1 Reporting</b> .....	5
<b>7.0 ASSOCIATED DOCUMENTS</b> .....	5
<b>8.0 APPROVAL</b> .....	6
<b>9.0 APPENDIX</b> .....	6

UNCONTROLLED WHEN PRINTED

14/12/2025

## **DEFINITIONS:**

### **Information Security Incident/Security Breach**

An Information Security Incident or Security Breach can be defined as any event that poses a potential, suspected or actual threat to the security, confidentiality, integrity, or availability of the personal data processed by NMLS. Information Security Incidents/Security Breaches can include:

- Intentional or accidental disclosure of any personal data processed by NMLS, in particular data of a confidential, high risk or sensitive nature, to anyone not authorised to view it;
- Loss or theft of paper records, data or equipment such as files, tablets, laptops or smartphones on which personal data is stored;
- The execution of a malicious program designed to infiltrate and damage computers without the user's consent (e.g. malware or viruses from clicking on links or attachments in e-mails or from visiting compromised websites);
- Denial of service attacks (e.g. deliberate attempts to interrupt or suspend services of a host connected to the Internet);
- Security attacks on IT equipment systems or networks (e.g. hacking, malware and ransomware); and
- Breaches of physical security that pose the threat of unauthorised access to sensitive personal data.

### **Incident Response Team (IRT)**

For the purposes hereof, IRT means all HoDs, Supervisors, and Information Technology Personnel tasked by the Principal with the responsibility of identifying, monitoring, controlling, managing, and reporting on potential or actual data breaches within or connected to the organisation.

### **Information Technology**

Systems (especially those related to computers and telecommunication) for storing, retrieving, and sending information.

UNCONTROLLED WHEN PRINTED.

Revision Date: July 18, 2024

ii  
July 18, 2024  
14/5/2025

### **Information Security**

The preservation of the confidentiality, integrity and availability of information, whether in a physical or digital form.

### **Unauthorised Access**

Refers to individuals gaining access to the NMLS's data, networks, endpoints, applications, devices, files (both physical and electronic), or sensitive material without permission.


**Table 1. List of Acronyms/ Abbreviations**

<b>Initialisms/Acronyms</b>	<b>Meaning</b>
DPA	Data Protection Act, 2020
DPO	Data Protection Officer
HoD's	Head of Department
IT	Information Technology
NMLS	The Council of Legal Education – Norman Manley Law School
IRT	Incident Response Team
IRP	Incident Response Policy
OIC	Office of the Information Commissioner

MS 14/5/2025



## NORMAN MANLEY LAW SCHOOL

	DEPARTMENT/UNIT: Office of the Principal	DOCUMENT NO: PDIR/OOP/01	Page 1 of 6
	TITLE: Personal Data Incident Response Policy (PDIR)	REVISION NO.: 00	REVISION DATE: March 13, 2025

### 1.0 TITLE: Personal Data Incident Response Policy

### 2.0 POLICY STATEMENT

The effective and secure management of personal data is crucial to ensuring that The Council of Legal Education - Norman Manley Law School (NMLS) can efficiently conduct its business and meet its obligations under the Data Protection Act (DPA).

All users of personal data processed by NMLS have a responsibility to:

- a) complete all mandatory training on Data Protection and Information Security.
- b) minimise the risk of information being lost or disclosed to unauthorised individuals.
- c) protect the security and integrity of IT systems or devices on which personal data is held or processed.
- d) ensure that physical security measures for protecting sensitive information are adequate and
- e) report actual or suspected information security incidents promptly so that appropriate action can be taken to mitigate risks and minimise potential harm to data subjects and to NMLS.

### 3.0 PURPOSE


This policy explains the actions required in the event of an Information Security Incident involving personal data and sets out the responsibilities of all users of the personal data processed by NMLS with respect to reporting and managing incidents.

In the event of an actual (or suspected) information security incident or security breach involving personal data, NMLS must take prompt action to mitigate the risks of potential harm to individuals, damage to operational business, and financial, legal and reputational costs. Where

UNCONTROLLED WHEN PRINTED.

*Handwritten signature and date:*  
14/5/2025

## NORMAN MANLEY LAW SCHOOL

	DEPARTMENT/UNIT: Office of the Principal	DOCUMENT NO: PDIR/OOP/01	Page 2 of 6
	TITLE: Personal Data Incident Response Policy (PDIR)	REVISION NO.: 00	REVISION DATE: March 13, 2025

information security incidents are not reported, or where reports are delayed, the consequences can be severe and include:

- a) damage or disruption to organisational systems;
- b) damage and distress to individuals;
- c) significant monetary penalties levied by the Office of the Information Commissioner (OIC);
- d) custodial sentences against officers of NMLS;
- e) harm to NMLS' reputation and subsequent erosion of trust;
- f) loss of business assets;
- g) increased risk of fraud or identity theft.

### 4.0 SCOPE

**4.1** This policy forms part of NMLS' Incident Management Policy. Overall responsibility for the policy lies with the Principal.


**4.2** This policy applies to:

- a) all personal data processed by NMLS in any format, whether held on-premise or remotely, stored on desktop or static devices, or portable devices and media, whether transported from the workplace physically and electronically or accessed remotely;
- b) any incident that could have a detrimental effect on any of NMLS' information assets or systems;
- c) all users of personal data processed by NMLS, including heads of department (HoDs), employees (permanent, contract, temporary and casual), contractors working on behalf of NMLS, students and third parties;
- d) all NMLS-owned and managed IT systems;
- e) any NMLS IT systems on which personal data is held or processed, including personally owned devices;

UNCONTROLLED WHEN PRINTED.

*Handwritten signature and date:*  
14/5/2025

## NORMAN MANLEY LAW SCHOOL

	DEPARTMENT/UNIT: Office of the Principal	DOCUMENT NO: PDIR/OOP/01	Page 3 of 6
	TITLE: Personal Data Incident Response Policy (PDIR)	REVISION NO.: 00	REVISION DATE: March 13, 2025

- f) all locations at which personal data processed by NMLS is held, including locations outside of Jamaica.

### 5.0 PROCEDURE

IRP and reporting mechanisms will be communicated to all personnel.


- a) Information Security Incidents/Security Breaches should be reported through the appropriate management channels as quickly as possible.
- b) Personnel and contractors using NMLS' information systems and services are required to note and report any observed or suspected security weakness, vulnerability in the systems or services, Information Security Incident or Security Breach.
- c) An Information Security Incident/Security Breach should be responded to in accordance with NMLS' documented *Personal Data Breach Notification Procedure*.
- d) NMLS must report any security breach in respect of its operations which affects or may affect personal data to the Information Commissioner within seventy-two (72) hours of becoming aware of the security breach.
- e) NMLS must also notify each data subject whose personal data is affected by the security breach within seventy-two (72) hours of becoming aware of or having reason to become aware of the breach of the nature of the security breach, the measures taken to mitigate the possible adverse effects of the breach and the contact information of its data protection officer.
- f) Knowledge gained from analysing and resolving an Information Security Incident/Security Breach should be used to reduce the likelihood or impact of future incidents.
- g) Procedures should be defined and applied for the identification, collection, acquisition, and preservation of information related to an information security incident/breach, which can serve as evidence.

UNCONTROLLED WHEN PRINTED.

*Handwritten signature and date:*  
14/5/2025



## NORMAN MANLEY LAW SCHOOL

	DEPARTMENT/UNIT: Office of the Principal	DOCUMENT NO: PDIR/OOP/01	Page 4 of 6
	TITLE: Personal Data Incident Response Policy (PDIR)	REVISION NO.: 00	REVISION DATE: March 13, 2025

### 6.0 RESPONSIBILITIES

- All users of personal data processed by NMLS are responsible for reporting information security incidents/security breaches. This includes actual, potential, and suspected incidents.
- The Incident Response Team (IRT) is responsible for ensuring that all users of personal data processed by NMLS are made aware of this policy and for assisting with any investigations or incident management response as required.
- The Principal/DPO has overall responsibility for Incident Response policies, procedures and training.

The Principal/DPO is responsible for:

the communication and management of reports on Information Security Incident/Security Breaches;

- maintaining a central record of incidents reported and actions taken;
- advising on mitigating steps,
- changes to current practices and making best practice recommendations;
- co-ordination of incidents referred to the IRT and
- advising on and completing notifications to the Office of the Information Commissioner (OIC).

#### 6.1 Compliance/Monitoring/Review

The Principal/DPO will ensure that the relevant departments, supervisors and HoD's are equipped to respond effectively and efficiently to cyber incidents or threats.

In order to achieve this the following activities will be undertaken:


- Simulation exercises every six (6) months.
- Training exercises on an annual basis and for newly onboarded staff.
- Regular reporting on and review of incidents.

UNCONTROLLED WHEN PRINTED.

*MS*  
14/5/2025



## NORMAN MANLEY LAW SCHOOL

	DEPARTMENT/UNIT: Office of the Principal	DOCUMENT NO: PDIR/OOP/01	Page 5 of 6
	TITLE: Personal Data Incident Response Policy (PDIR)	REVISION NO.: 00	REVISION DATE: March 13, 2025

- d) Inclusion of training requirements in individual workplans.
- e) Review of departmental procedures six (6) months before the review of operational plans to ensure that all staff and in particular HoD's and Supervisors are able to comply with the DPA.

### 6.1.1 Reporting

The Principal/DPO shall report on the implementation and effectiveness of this policy at the regularly scheduled meetings of the HoD's and bi-annually at the general staff meeting.

### 6.1.2 Records Management

All HoDs and line managers must maintain all records relevant to administering this Policy in a secure recordkeeping system. Documents must be easily retrievable and disposed of in accordance with the NMLS document retention schedule.

## 7.0 ASSOCIATED DOCUMENTS

NMLS Information Security Policy/ ICT Policy


NMLS Document Retention Schedule

Personal Data Incidence Breach Notification Manual

*Handwritten signature and date: 14/5/2025*

UNCONTROLLED WHEN PRINTED.

## NORMAN MANLEY LAW SCHOOL

	DEPARTMENT/UNIT: Office of the Principal	DOCUMENT NO: PDIR/OOP/01	Page 6 of 6
	TITLE: Personal Data Incident Response Policy (PDIR)	REVISION NO.: 00	REVISION DATE: March 13, 2025

### 8.0 APPROVAL

*Julius*

Current Document Revision #:	Rev 00
Revision Date:	March 13, 2025
Procedure Owner:	Office of the Principal
Approval Authority & Date:	14/5/2025 <i>Julius</i>
Next Revision Date/Period:	March 2028
Document Revision Note:	

### Revision History

Last Revision #:	
Last Revision Date:	
Change Summary:	

### 9.0 APPENDIX

UNCONTROLLED WHEN PRINTED.