DATA SECURITY POLICY

Version number	Date approved (including committee)	Reason for production/revision	Author	Proposed next review date
V1.1	IGG Sept 2023	Periodic review	Business Development Director	Q1 25-26
V1.0	Sept 2021 ExCo	Replacing the Manual and alignment with the Information Governance Framework	Business Development Director	Biennially and as required
Related policies				
Data Protection Policy Freedom of Information Policy Employee Records Data Protection Policy Records Management Policy Email Use Policy Acceptable Us of IT Policy Bring Your Own Device Policy Business Continuity Policy Staff Disciplinary Policy Student Disciplinary Policy Equality & Diversity Policy Safeguarding Policy				
External Reference				
General Data Protection Regulation (GDPR), UK GDPR, the Data Protection Act 2018 and the Privacy and Electronic Communications Regulation (PECR),				

1. INTRODUCTION

1.1. ICMP is reliant on its information assets (also known as data assets) to function effectively. It is essential that ICMP's information assets are protected against the consequences of breaches of confidentiality, failures of integrity and interruptions to availability. An information security breach could damage ICMP's reputation, cause distress to individuals, and result in substantial fines from the Information Commissioner's Office (ICO).

2. PURPOSE

The purpose of this Policy is to:

2.1. set out ICMP's intentions in managing information security as part of effective information governance

2.2. ensure the protection of all ICMP's information assets and to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these assets

2.3. ensure that ICMP's authorised users are aware of and are in a position to comply with all current and relevant UK and EU legislation

2.4. ensure that ICMP's authorised users understand their own responsibilities for protecting, preserving and managing the confidentiality, integrity and availability of ICMP's information assets

2.5. set out ICMP's intentions in managing information security as part of effective governance

3. SCOPE

This Information Security Policy:

3.1. Applies to all staff, students, directors, consultants, contractors, partnership organisations and partner staff of ICMP

3.2. Covers all information handled, stored, processed or shared by ICMP irrespective of whether that information originates with or is owned by ICMP

3.3. Applies to all computer and non-computer based information systems owned by ICMP or used for ICMP business or connected to ICMP managed Networks

3.4. ICMP's **Information Classification and Handling Scheme** provides guidance on the classification of information and the different levels of security required.

3.5. It encompasses **all information** held by ICMP, in any format (electronic and hard-copy).

3.6. Information is classified by Information Asset Owners as **Public, Restricted or Classified.** Once classified the scheme specifies appropriate security measures to

be implemented by the Information Owner.

3.7.

4. POLICY

Data Security principles:

4.1. Information assets are identified, classified and protected in accordance with the Information Asset Register (IAR) documentation. Any security controls which are implemented must be proportionate to the defined classification. Information assets are controlled by the Information Asset Owners as outlined in the Information Governance Framework document and in the IAR.

4.2. All of ICMP's information assets whether electronic or in hard-copy form must be protected against unauthorised access

4.3. ICMP's information assets must be available to all those who have a legitimate need to access them

4.4. The integrity of ICMP's information must be maintained so that it is accurate and complete

4.5. All users of ICMP's information systems will comply with ICMP's Information Governance Framework, and all of the policies, procedures and guidance contained therein, such as data security,data protection and ITpolicies. It is the responsibility of users to ensure that they continually familiarise themselves with and fully understand the contents of framework and its policies and guidance. Failure to comply with the information security policies and guidance may result in disciplinary action.

4.6. All users of ICMP's information systems will abide by and adhere to all current UK and EU legislation as well as regulatory and contractual requirements

4.7. All information assets will be classified according to their required levels of confidentiality as within the Information Classification and Guidance Scheme. The classification of the asset will determine the security controls that will be applied to it and how it must be handled. The classification will be recorded in the IAR.

4.8. All information assets will be assigned an owner who will be responsible for ensuring that the asset has the correct information classification, has adequate protection and is handled at all times in accordance with its classification.

4.9. Key information assets will be subject to annual risk assessments to identify the probability and impact of security failures. The results of the risk assessments will determine the appropriate security controls to be applied to the assets. Key Information assets are identified in the IAR and the risk assessments are recorded within relevant Operational Risk Registers.

4.10. All users of ICMP's information systems shall receive information security training appropriate to their role.

4.11.   All suspected and actual information security breaches must be recorded and reported through the DPO by completing a 'helpdesk' ticket or via email at dataprotection@icmp.ac.uk.

5. TRAINING

5.1. Annual Information Security training is mandated by the Executive Committee and therefore must be undertaken by all staff, contracted or FTE. If the contracted staff have completed a suitable level of security training elsewhere, ICMP will accept a certificate on submission to the HR team. Information regarding the provision of the training and the monitoring and recording of completion will be managed by the HR department.

5.2. The HR department provide an annual report to the IGG and Executive Committee detailing completion rates and therefore provide assurance regarding ICMP's plans and mitigating actions.

6. SUPPORTING GUIDANCE AND PROCEDURES

6.1. The following documents, whilst not included in this policy document provide the wider clarification of Information Security and therefore the same levels of application and adherence are required and expected to ensure a fully robust Information Security environment.

6.1.1. Data Classification and Handling Guidance

6.1.2. Clear Desk and Screen Policy

6.1.3. Information Security Risk Management Guidance

6.1.4. IT Monitoring and Interception Guidance

6.1.5. Mobile Device Guidance

6.1.6. Bring Your Own Device Policy

6.1.7. Removable Media Guidance

6.1.8. Third Party Access for Staff Guidance

6.1.9. IT Guidance (supplement to the Acceptable Use of IT Policy)

6.1.10. Two Factor Authentication Guidance

6.1.11. Password Management Guidance

7. PROCEDURES

7.1. A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data are lost, destroyed, corrupted or disclosed; if someone accesses the data or passes them on without proper authorisation; or if the data are made unavailable, for example, when they

have been encrypted by ransomware, or accidentally lost or destroyed.

7.2. ICMP will ensure that all of its employees, contractors, agents, consultants, partners, or other parties working on behalf of ICMP comply with ICMP's Information Classification and Handling Scheme which specifies the levels of security and encryption when processing information.