POLICY / PROCEDURE TITLE		DATE OF APPROVAL
NCG Data Classification Policy		February 2024
APPROVED BY	**VERSION NO.**	**VALID UNTIL**
Executive Board	1.4	February 2025

OWNER	IT Security Lead
GROUP EXECUTIVE LEAD	CIDEO
DOCUMENT TYPE	Policy ☒ Group Procedure ☐ Local Procedure ☐
PURPOSE	The purpose of this policy is to define the data security classification of NCG data.
APPLICABLE TO	All users who have access to NCG networks and systems.
EQUALITY ANALYSIS COMPLETED [POLICIES ONLY]	Yes ☒ No ☐ N/A ☐
	(If EA not applicable, please explain)
KEY THINGS TO KNOW ABOUT THIS POLICY	1. **EMPLOYEES** are allowed to send or communicate an unclassified piece of data with anyone inside or outside of the organisation. This data may be saved to removable media and transported without the need for password protection or encryption. 2. **PRIVATE** data is defined as corporate information that is to be kept within the organisation. Access to this data may be limited to specific departments and cannot be distributed outside of the workplace. 3. **OFFICIAL** data includes the majority of information that is created or processed by NCG for internal or external use which is not classified as PRIVATE. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile.
EXPECTED OUTCOME	Readers are expected to understand the organisational position on data classification, know their responsibilities in relation to the policy and comply with the terms of the policy.

MISCELLANEOUS	
LINKED DOCUMENTS	• N/A
KEYWORDS	• Data • Classification

	• Legislation

Equality Impact Assessment

EQUALITY IMPACT ASSESSMENT	Yes	No	Explanatory Note if required
EIA 1 - Does the proposed policy/procedure align with the intention of the NCG Mission and EDIB Intent Statement in Section 2?	☒	☐	The answer to this must be YES
EIA 2 - Does the proposed policy/procedure in any way impact unfairly on any protected characteristics below?	☐	☒	
Age	☐	☒	The answer to this must be NO
Disability / Difficulty	☐	☒	The answer to this must be NO
Gender Reassignment	☐	☒	The answer to this must be NO
Marriage and Civil Partnership	☐	☒	The answer to this must be NO
Race	☐	☒	The answer to this must be NO
Religion or Belief	☐	☒	The answer to this must be NO
Sex	☐	☒	The answer to this must be NO
Sexual Orientation	☐	☒	The answer to this must be NO
EIA3 - Does the proposed policy/processes contain any language/terms/references/ phrasing that could cause offence to any specific groups of people or individuals?	☐	☒	The answer to this must be NO
EIA4 - Does the policy/process discriminate or victimise any groups or individuals?	☐	☒	The answer to this must be NO
EIA 5 - Does this policy/process positively discriminate against any group of people, or individuals?	☐	☒	The answer to this must be NO
EIA 5 - Does this policy/process include any positive action to support underrepresented groups of people, or individuals?	☐	☒	The answer to this could be yes or no as positive action is lawful. However, an explanation must be provided for clarity.
EIA 6 - How do you know that the above is correct?	This is 'reality check' question to ensure that this is not a simple box ticking exercise. A simple way of ensuring that this is the case is to ensure that the policy/process author has consulted with peers and appropriate groups of people in the Group. As a general rule, the wider the reach and potential impact of the Policy the wider the consultation.		

1. **GENERAL POLICY STATEMENT**

    This document defines the data security classification of NCG data. Its purpose is to inform employees of NCG of the rules and procedures relating to data security compliance. NCG is responsible for the security and integrity of all data that it holds and must protect this data using all means necessary by ensuring data is classified accordingly and protected in accordance with the classification guidelines.

2. **SCOPE**

    It is the responsibility of everyone who works within NCG to protect its data. Even unintentional abuse of classified data will be considered punishable in accordance with the extent and frequency of the abuse.

    The data covered by this policy includes but is not limited to all electronic information found in NCG Information Processing assets; paper information, such as hard copies of electronic data, employee files, internal memos and any other such information.

    This scheme is for the internal classification of data and is not intended to interfere with, but to work in conjunction with the Data Protection and Freedom of Information acts.

    Any individual wishing to request their personal data in accordance with the Data Protection Act and individuals wishing to request official information under the Freedom of Information Act should contact the Chief Operations & Compliance Officer and Secretary to the Board or nominated representative.

    Should any member of staff be asked to supply data under either the Freedom of Information or Data Protection Acts, they should refer the request to the Chief Operations & Compliance Officer and Secretary to the Board or nominated representative without delay.

3. **DATA CLASSIFICATIONS**

    The Government Security Classifications policy classifies data into three categories; OFFICIAL, SECRET and TOP SECRET. NCG has adopted this

classification scheme however does not have a responsibility for any data that is classified above OFFICIAL.

PUBLIC/UNCLASSIFIED – Despite the Government Protective Marking Scheme not having a tier that sits below OFFICIAL, NCG considers PUBLIC/UNCLASSIFIED information to be information that is generally available to anyone within or outside of the organisation. Access to this data is unrestricted, may already be available and can be distributed as needed. Unclassified data includes but is not limited to marketing materials. Employees may send or communicate an unclassified piece of data with anyone inside or outside of the organisation.

This data may be saved to removable media and transported without the need for password protection or encryption.

PRIVATE - This is defined as corporate information that is to be kept within the organisation. Access to this data may be limited to specific departments and cannot be distributed outside of the workplace. Private data includes, but is not limited to, work phone directories, organisational charts, company policies and other data as applicable.

OFFICIAL - The majority of information that is created or processed by NCG for internal or external use which is not classified as PRIVATE. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile. Official data includes, but is not limited to, work phone directories, organisational charts, company policies and other data as applicable. In addition, the day to day business of NCG service delivery, many aspects of security and resilience, commercial interests including information provided in confidence and intellectual property, personal information that is required to be protected under the Data Protection Act or other legislation (e.g. health records, social security numbers, contact information, tax forms, accounting data), security procedures and other data as applicable. NCG considers it a top priority to protect the privacy of our clients and employees.

4. RELEVANT RELATED LEGISLATION

- Data Protection Act 2018
- EU General Data Protection Regulations (EU2018/1725)
- Computer Misuse Act 1990

5. RESPONSIBILITIES

- All employees are responsible for adhering to the policy and reporting any activities that do not comply with this policy.
- Management is responsible for ensuring that their direct reports understand the scope and implications of this policy.
- IT staff will be monitoring data for any unauthorized activity and are responsible for updating access requirements as needed.
- Any employee who authors or generates corporate or client data must classify that data according to the criteria outlined above.
- Each data share will be required to have a data owner, who has overarching oversight and responsibility for the information within that share.
- Each data share can also have up to 3 access control approvers.
- These approvers will be specified by the data owner. They will be contacted by the Group Helpdesk in the event that someone requests access to a data share to confirm that the access request is valid.
- Each month the IT Operations teams will send a report to the data owners advising them of the current share access membership for the data owners to confirm access is appropriate.
- These are the accepted technologies NCG use to enforce and ensure data security:

  - Access controls
  - Strong passwords
  - Encryption
  - System monitoring
  - Audit

6. STATEMENT ON POLICY IMPLEMENTATION

Upon approval, this policy will be uploaded to the policy portal and communicated to staff via The Business Round-Up.

7. STATEMENT ON EQUALITY AND DIVERSITY

NCG is committed to providing equality of opportunity. Further details or our aims and objectives are outlined in our [Equality Diversity Inclusion and Belonging Strategy](#).

This policy has been assessed to identify any potential for adverse or positive impact on specific groups of people protected by the Equality Act 2010 and does not discriminate either directly or indirectly. In applying this policy, we have considered eliminating unlawful discrimination, promoting equality of opportunity and promoting good relations between people from diverse groups.

8. STATEMENT ON CONSULTATION

This policy has been reviewed in consultation with Information and Data Services team and subsequently with members of the Policy Review Council as part of the policy review and approval process.

VERSION CONTROL				
Version No.	Documentation Section/Page No.	Description of Change and Rationale	Author/Reviewer	Date Revised
1.0		Annual review and update	N/A	07/05/15
1.1		Annual review and update	N/A	18/07/16
1.2		Review and update for new legislation	N/A	02/05/18
1.3		Annual review and update	Director IDS	05/09/22
1.4		Annual review and update to new template.	Director IDS	17/01/24