POLICY / PROCEDURE TITLE		DATE OF APPROVAL
Information Governance Policy		May 2024
APPROVED BY	**VERSION NO.**	**VALID UNTIL**
Executive Board	3	May 2027

OWNER	Director of Assurance and Risk		
GROUP EXECUTIVE LEAD	Chief Finance Officer		
DOCUMENT TYPE	Policy ☒ Group Procedure ☐ Local Procedure ☐		
PURPOSE	The purpose of this policy is to establish the high-level principles, set out responsibilities for staff and provide a framework of Information Governance across NCG.		
APPLICABLE TO	All NCG employees, as well as consultants, vendors, agency workers, contractors, service users, trainees/students, volunteers and/or any other parties who have a business relationship with NCG.		
EQUALITY ANALYSIS COMPLETED [POLICIES ONLY]	Yes ☒	No ☐	N/A ☐
	(If EA not applicable, please explain)		
KEY THINGS TO KNOW ABOUT THIS POLICY	1. Clarity on roles and responsibilities in relation to information governance 2. Identifies underpinning legislation and regulations. 3. Sets out objectives and purpose of an information governance framework		
EXPECTED OUTCOME	Readers are expected to understand the organisational position on Information Governance and know their responsibilities in relation to the policy and comply with the terms of the policy.		

MISCELLANEOUS	
LINKED DOCUMENTS	• Information Governance Policy. • Data Protection Policy. • Special Category and Criminal Conviction Data Policy. • Records Retention Schedule. • Information Security Policy. • Acceptable Use Policy.

	• Freedom Of Information (FOI) And Environmental Information Regulations (EIR) Policy
KEYWORDS	• Information Governance • Framework • Third Party • GDPR • Data Protection

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?	☒	☐	
EIA 2 - Does the proposed policy/procedure in any way impact unfairly on any protected characteristics below?	☐	☒	
Age	☐	☒	
Disability / Difficulty	☐	☒	
Gender Reassignment	☐	☒	
Marriage and Civil Partnership	☐	☒	
Race	☐	☒	
Religion or Belief	☐	☒	
Sex	☐	☒	
Sexual Orientation	☐	☒	
EIA3 - Does the proposed policy/processes contain any language/terms/references/ phrasing that could cause offence to any specific groups of people or individuals?	☐	☒	
EIA4 - Does the policy/process discriminate or victimise any groups or individuals?	☐	☒	
EIA 5 - Does this policy/process positively discriminate against any group of people, or individuals?	☐	☒	
EIA 5 - Does this policy/process include any positive action to support underrepresented groups of people, or individuals?	☐	☒	
EIA 6 - How do you know that the above is correct?	This policy has been reviewed in consultation with the Policy Review Council prior to being reviewed by Executive Board.		

1. GENERAL POLICY STATEMENT

NCG is committed to protecting staff and student data and managing its information securely, legally and effectively to provide the best possible services to our staff and students. This document provides clear guidance to staff around how information should be managed and outlines the accountability structures, governance processes, related policies & procedures, staff training and resources required to undertake this task.

2. SCOPE AND PURPOSE

The purpose of this document is to provide a framework for the handling of information at NCG to ensure regulatory and statutory compliance and to ensure the appropriate use of timely and accurate information assists in the delivery of NCG's Strategic Objectives.

The policy applies to all NCG staff as well as those working on behalf of NCG. It applies to the management and governance of all information across NCG with a particular emphasis on personal and confidential information. It applies to information held in both electronic and paper format and their associated systems. The policy sets out the procedures for sharing information with stakeholders, partners and suppliers.

3. OBJECTIVES

Through an Information Governance framework NCG aims to develop an information governance culture that will ensure all staff understand and apply information governance standards and principles on a consistent basis. Its key objectives are to:

- Ensure that NCG has a full suite of information governance policies and procedures to set the strategic direction and facilitate compliance with information governance requirements.
- To deliver training and promote colleague awareness of their information governance responsibilities.

- To control the retention and storage of data so that it can be accessed, controlled, managed, monitored, stored, preserved, and audited.
- To ensure the Group has accurate, trusted, and reliable records, data that management can confidently use to make informed decisions and report on accurately.
- To ensure the Group's information is secure and protected from loss and / or damage (including where there is third party involvement).
- To reduce the Group's risk of non-compliance with legislation and regulatory requirements by adopting the ICO's Accountability Framework as a fundamental part of NCG approach to compliance.

4. REGULATORY ENVIRONMENT

NCG is a data controller with obligations set out in the UK General Data Protection Regulation and Data Protection Act 2018. NCG is also a public authority with obligations under the Freedom of Information Act 2000.

The legal and regulatory framework for records management is outlined below and includes:

- Data Protection Act 2018.
- UK GDPR.
- Freedom of Information Act 2000.
- Environmental Information Regulations 2004.
- Computer Misuse Act 1990.

Related guidance and codes of best practice include:

- The ICO's published guidance.
- ISO Standards.
- Payment Card Industry Data Security Standard (PCI-DSS).
- Cyber Essentials Scheme.

5. ROLES AND RESPONSIBILITIES

Corporation

Corporation has overall responsibility for data protection and information governance, and for seeking assurance over the effectiveness of the operations in place to manage the associated risks.

Executive Board

Executive Board is responsible for strategically directing NCG and, as such, will ensure NCG has appropriate information governance procedures in place to mitigate risk and maximise the value of the information it holds.

Senior Information Risk Owner (SIRO)

The Chief Finance Officer is NCG's SIRO and has responsibility for:

- Providing updates to Corporation and Executive Board on compliance with legislation relating to data and information.
- Championing NCG's information governance policies and associated procedures.
- Maintaining strategic oversight of NCG's information risks and information risk assessment processes.

Data Protection Officer (DPO) and supporting team

The Data Protection Officer has responsibility for:

- Providing advice and guidance to colleagues to facilitate compliance with data protection legislation and best practice.
- Developing and delivering formal cross-organisation training to all staff (mandatory training and ad-hoc training as required).
- Developing a programme of assurance activity to monitor compliance with data protection requirements.
- Overseeing and owning the process to respond to Data Subject Access Requests.
- Responding to information incidents as they arise and reporting on the outcomes.

- Liaising with the ICO and for individuals whose data is being processed by the NCG (employees, customers, students etc.)
- Providing expert advice and assistance to the organisation and for putting the requirements of the Information Governance Framework into practice.
- Working with key staff within the business to establish information governance across NCG. This will also include:
    - Managing the Information Security Incident procedure.
    - Developing and implementing Data Protection, Information Governance and other related policies and procedures.
    - Managing information governance risk management activities (For example the Data Protection Impact Assessments).
    - Developing Data Processing Agreements and reviewing contract arrangements with third party organisations and suppliers
    - Staff training and awareness.

<u>Records Management Officer</u>

The Records Management Officer is responsible for:

- Oversight of NCG's management of physical and electronic records.
- Providing advice and guidance to colleagues to facilitate compliance with records management, information governance and best practice.
- Developing and delivering training to staff across NCG as appropriate.
- Oversight / Control of all onsite storage, and liaison with external storage providers (including regular review of storage costs and identification of cost efficiencies).
- Implementation and maintenance of NCG's Publication Scheme.

<u>Managers</u>

All managers and supervisors have responsibility for:

- Ensuring information governance policies, procedures and guidance notes are read and understood by their staff.
- Actively monitoring the regular training reports to confirm staff have completed their mandatory information security training every three years.

- Encouraging the safe handling of information by their staff and report any concerns about practice to the Information Governance Team.
- Reporting any information security incidents, they are made aware of to the Information Governance Team.

Staff

All staff have responsibility for:

- Reading and understanding NCG's information governance policies, procedures and guidance notes and contacting their manager if they require any clarification, advice and guidance.
- Completing their mandatory information security training every three years.
- Ensuring they are handling personal information in line with the NCG's policies and procedures and report any concerns about practice to the Information Governance Team.
- Reporting any information security incidents to the Information Governance Team.

6. INFORMATION POLICIES

NCG has established a framework of policies that cover Information Governance, Information Security, Data Protection and Freedom of Information.

- Information Governance Policy.
- Data Protection Policy.
- Special Category and Criminal Conviction Data Policy.
- Document Retention Schedule.
- Information Security Policy.
- Acceptable Use Policy.
- Freedom Of Information (FOI) And Environmental Information Regulations (EIR) Policy.
- Records Management Policy.

7. DISCLOSURE OF INFORMATION

Personal Data and Special Category Data shall not be disclosed other than in compliance with Data Protection legislation or another legal or contractual obligation.

Confidential Information shall not be disclosed except under NCG's or an equivalent Non-disclosure Agreement.

Corporate Information shall be disclosed through NCG's publication scheme.

8. WORKING WITH THIRD PARTIES

It is essential to establish how the organisation operates and shares information with stakeholders, partners and suppliers. Our approach for working with third parties is set out below.

<u>Third party supplier agreements and contracts</u>

NCG's procurement procedures mandate confirmation that a third-party supplier has the appropriate security and technical measures in place to protect NCG's personal and business information.

The Contracts and Procurement team ensures that any contract or agreement entered into with a third-party supplier has the appropriate contract or data processing agreement in place that outlines the information governance requirements prior to any information being shared.

<u>Information sharing with other organisations</u>

Information sharing shall be managed in accordance with NCG's data sharing protocols to ensure information sharing is managed in line with the organisation's legal duties and is carried out in a secure manner.

Information is shared on a strictly 'need to know' basis with only the minimum amount of information required being shared.

The detailed requirements for sharing data with other organisations are set out in the Data Protection Policy.

9. TRAINING AND GUIDANCE

All new staff receive awareness training and information on Information Governance, which includes Data Protection, Information Security and Freedom of Information. This mandatory training is repeated every three years.

Mandatory training compliance is monitored and reported in the weekly Mandatory Training Report and monthly dashboards circulated to senior management.

Support is available to all NCG colleagues via dpo@ncgrp.co.uk.

10. INCIDENT MANAGEMENT

All information security incidents and near misses must be reported immediately to the Data Protection Officer via dpo@ncgrp.co.uk

Examples of Information Security Incidents include:

- Personal data disclosed by misdirected e-mails or letters.
- Information being lost or stolen.
- Unauthorised access to systems or information.
- Successful phishing attacks where staff disclose network credentials.

11. MEASUREMENT AND REVIEW

A programme of assurance assignments to monitor compliance with this policy are undertaken (led by the Director of Assurance & Risk).

12. STATEMENT ON IMPLEMENTATION

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

13. 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.

14. STATEMENT ON CONSULTATION

This policy has been reviewed in consultation with the Policy Review Council prior to being reviewed by Executive Board.

VERSION CONTROL				
Version No.	**Documentation Section/Page No.**	**Description of Change and Rationale**	**Author/Reviewer**	**Date Revised**
1	New Policy	Initial release	Director of Assurance & Risk	N/A
2	Annual Review	No material changes	Director of Assurance & Risk	April 2023
3	Annual Review	Transferred to new template No material changes	Director of Assurance & Risk	April 2024