Policy Title	NCG Information Governance Policy (IGP-01)
Policy Category	Compliant
Owner	Director of Assurance & Risk
Group Executive Lead	Chief Operations & Compliance Officer
Date Written	March 2022
Considered By	Executive Board
Approved By	Corporation
Date Approved	May 2023
Equality Impact Assessment	The implementation of this policy is not considered to have a negative impact on protected characteristics
Freedom of Information	This document will be publicly available through the Group's Publication Scheme.
Review Date	May 2024
Policy Summary	This policy sets out NCG's commitment to achieving high standards in Information Governance. It establishes the high-level principles, sets out responsibilities for staff and provides a framework of Information Governance across NCG.

Applicability of Policy	Consultation Undertaken	Applicable To
Newcastle	No	Yes
Newcastle Sixth Form	No	Yes
Carlisle	No	Yes
Kidderminster	No	Yes
Lewisham	No	Yes
Southwark	No	Yes
West Lancashire	No	Yes
Professional Services	No	Yes

Changes to Earlier Versions	
Previous Approval Date	**Summarise Changes Made Here**
N/A	Initial release
April 2023	Annual review – No material changes
Linked Documents	
Document Title	**Relevance**
Data Protection Policy	Directly relates to the operation of this document.
Information Security Policy	Directly relates to the operation of this document.
FOIA and EIR Policy	Directly relates to the operation of this document.

1. Introduction

Information Governance describes the holistic approach to managing information by implementing processes, roles and metrics to manage the processing of information and transform information into a business asset. The purpose of this policy is to formally establish NCG's approach to Information Governance.

2. 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.

3. Scope and Purpose

NCG is a data controller with obligations set out in the UK GDPR and Data Protection Act 2018 and a public authority with obligations under the Freedom of Information Act 2000. The purpose of this document is to provide a framework for the handling of information in NCG to ensure regulatory and statutory compliance and to ensure that appropriate use of timely and accurate information assists in the delivery of the 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. It sets out the procedures for sharing information with stakeholders, partners and suppliers.

4. 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, has data that management can confidently use to make informed decisions and report on accurately.

- To ensure the Group's information is secure and is 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.

5. Regulatory Environment

NCG is a data controller with obligations set out in the UK GDPR & Data Protection Act 2018 and 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 General Data Protection Regulation.
- 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.

6. 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 Operations & Compliance 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.
- 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 Information Asset Owners (see definition below) and key staff within the business to establish information governance across NCG. This will also include:
    - Managing the Information Security Incident procedure.
    - Developing and implementing the Data Protection, Information Governance and other related policies and procedures.
    - Managing IG 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.

Information Asset Owners (IAOs)

Information Asset Owners are accountable for the information held within their area of the business and will have a clear understanding of how the information is held, used and shared.

The Information Asset Owners will also be responsible for promoting a culture of good information governance and for ensuring compliance with all IG requirements.

Information Asset Administrator (IAAs)

Designated by the relevant IAO, Information Asset Administrators are individuals with operational responsibility for specific information assets. They are staff members with expert knowledge of business processes and how data is used within those processes. As such they can identify and report any operational concerns or risks to IAOs to be escalated accordingly.

Managers

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 two 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 two 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.

7. 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.
- Records Retention Schedule.
- Acceptable Use Policy.
- FOI & EIR Policy.
- Records Management Policy

8. 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 publishing scheme.

9. 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 are set out below.

Third party supplier agreements and contracts

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.

Information sharing with other organisations

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.

10. Training and Guidance

Information Governance is a mandatory part of NCG's induction training. All new staff shall receive awareness training and information on Information Governance, which includes Data Protection, Information Security and Freedom of Information. This mandatory training shall be repeated every two years.

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

The NCG Information Governance Team are available to support all NCG colleagues and can be contacted via dpo@ncgrp.co.uk.

11. Incident Management

All information security incidents and near misses must be reported immediately to the Information Governance Team as per the Information Security Incident Reporting Policy.

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.

12. Measurement and Review.

The Information Governance team will develop a programme of Information Governance Reviews. Following the completion of a review, action plans will be agreed with IAOs and monitored until completed.