

# NCG Records Management Policy (IGP-09)



<b>Policy Title</b>	<b>Records Management Policy (IGP-09)</b>	
<b>Policy Category</b>	Compliant	
<b>Owner</b>	Assistant Director Information Governance	
<b>Group Executive Lead</b>	Executive Director and Secretary to the Board	
<b>Date Written</b>	March 2022	
<b>Considered By</b>	Executive Board	
<b>Approved By</b>	Executive Board	
<b>Date Approved</b>	April 2022	
<b>Equality Impact Assessment</b>	The implementation of this policy is not considered to have a negative impact on protected characteristics	
<b>Freedom of Information</b>	This document will be publicly available through the Group's Publication Scheme.	
<b>Review Date</b>	April 2023	
<b>Policy Summary</b>	This policy sets out NCG's commitment to achieving high standards in Records Management and meeting its statutory obligations.	
<b>Applicability of Policy</b>	<b>Consultation Undertaken</b>	<b>Applicable To</b>
<b>Newcastle</b>	Yes	Yes
<b>Newcastle 6th Form</b>	Yes	Yes
<b>Carlisle</b>	Yes	Yes
<b>Kidderminster</b>	Yes	Yes
<b>Lewisham</b>	Yes	Yes
<b>Southwark</b>	Yes	Yes
<b>West Lancashire</b>	Yes	Yes
<b>Professional Services</b>	Yes	Yes
<b>Changes to Earlier Versions</b>		
<b>Previous Approval Date</b>	<b>Summarise Changes Made Here</b>	
N/A	New Document	
<b>Linked Documents</b>		
<b>Document Title</b>	<b>Relevance</b>	
NCG Document Retention Schedule	Sets out the retention periods for records and who is responsible for managing each record type.	
NCG Data Protection Policy	Sets out NCG's commitment to compliance with the Data Protection Principles including its approach to data sharing.	

## 1. Introduction

Information is an essential corporate asset and NCG's records are important sources of administrative and evidential information that support the work of the organisation.

Information Management is the systematic control over the lifecycle of records (Create > Use > Maintain > Destroy) and requires a business to have an established and embedded approach to records management that ensures it:

- Can access the required information to make informed decisions and to operate in an efficient and effective way.
- Meets business, regulatory, legal, contractual and accountability requirements.
- Protects the rights and freedoms of our students, staff and other associated third parties.
- Provides an audit trail to meet business, regulatory and legal requirements.
- Supports continuity and consistency in management and administration.

This policy sets out how NCG will manage its records and forms part of the NCG Information Governance Framework.

## 2. Definitions

Business documents fall into one of two categories, records and non-records:

- **Records** reflect the actions, decisions and obligations of NCG. They can exist in any media format and in different locations. Their legal, regulatory, business and / or historical significance make records subject to formal record keeping requirements, in line with the agreed Retention Schedule. A record can be defined as information created, received and maintained as evidence and information by an organisation, in pursuance of legal obligations or in the transaction of business.
- **Non-records** comprise disposable information including such items as:
  - Convenience copies – Documents copied to you as a convenience.
  - Working Documents – Short term records created as part of or in conjunction with working on a task.
  - Drafts – All earlier versions of a final record.
  - Transitory Information – Documents with no on-going business value. For example, notes, out-of-office messages, 'thanks' messages and personal e-mail.

In most cases there are no retention requirements for non-records and as a result they should be destroyed once they are no longer needed or have been superseded.

### 3. Scope

This policy applies to all records, digital or physical, that are created, maintained or received by NCG. It applies throughout the lifecycle of all records and across all storage locations and systems.

The policy applies to all staff, consultants, contractors or other third parties that are given access to our records.

### 4. Statutory and Regulatory Environment

NCG is committed to operating in a manner that ensures it remains compliant with its statutory, regulatory and contractual requirements. NCG is a data controller and a public authority with obligations under UK legislation including:

- Data Protection Act 2018.
- UK General Data Protection Regulation (UK GDPR).
- Freedom of Information Act 2000.
- Limitation Act.

Related guidance and code of good practice:

- Section 46 Freedom of Information Act - Records Management.
- ISO 15489 - Records Management.
- The ICO's published guidance and codes of practice.

### 5. Responsibilities

NCG has a corporate responsibility to maintain its records in accordance with the regulatory environment. All staff, contractors, consultants and any third party who creates, receives, maintains, or has access to our records are responsible for ensuring that they act in accordance with this document and other approved information governance policies and procedures. The Information Governance Policy (IGP-01) contains more details.

However, some staff have additional responsibilities in relation to the management of records as noted below.

- The Executive Director & Secretary to the Board is the Senior Information Risk Owner and as such has overall responsibility for ensuring business related records and non-records are controlled appropriately.
- The Assistant Director - Information Governance is responsible for establishing, embedding and assuring an appropriate framework under which the operational areas of the business will operate in alignment.

- Senior Post Holders are responsible for ensuring that their college / service area is operating in line with the guidance published.
- Information Asset Owners (IAO) should ensure a clear allocation of responsibility within each department or service area for the management of its records including identifying the appropriate retention period, defining, managing and monitoring suitable filing schemes and Management Rules for those records.

More generally, line managers are responsible for ensuring that their staff are aware of this policy and comply with its requirements. All members of staff are responsible for ensuring that their work is documented appropriately, the records that they create or receive are accurate and managed correctly and are maintained and disposed of in accordance with NCG's guidelines and any legislative, statutory and contractual requirements. Line managers should ensure that when a member of staff leaves, responsibility for their records is transferred to another person; if any of the information is redundant, it should be deleted by either the departing member of staff or their line manager.

It is vital that records management considerations are appropriately incorporated into project and planning processes and system design at the earliest possible stage of development. Where records contain personal data there is a legal requirement to do this to ensure that a Data Protection by Design and Default approach is followed.

### 6. Policy Statements and Standards

NCG is committed to managing its records in a manner that meets its statutory obligations. It is expected that NCG staff shall ensure that:

- Records shall be retained in accordance with the Records Retention Schedule.
- Non-records be kept no longer than necessary and shall be disposed of as soon as possible.
- When records have passed their retention period, as defined in the Records Retention Schedule, they shall be reviewed and where applicable destroyed.
- Records undergo appropriate destruction when no longer required, in an organised, efficient, timely and (where necessary) confidential manner.
- Records be managed and stored in a suitable format to retain quality, relevance, accessibility, durability and reliability. Any transfer to another format must ensure these elements are maintained.
- Records be kept with appropriate technical and administrative controls that reflect the confidentiality, nature and importance of the content.
- Records be managed via systems and processes ensuring efficiency and consistency throughout their lifecycle of creation, distribution, use, maintenance and destruction.

- Records be accurate, authentic, reliable, useable, timely and well-managed to demonstrate evidence, accountability and information about NCG's decisions and activities.
- Records be managed in a manner that fully meets NCG's legislative, statutory and contractual record-keeping obligations, including the Data Protection Act 2018 and the Freedom of Information Act 2000.

## 7. Rules for Records Management

### 7.1 Creation of Records

All NCG departments shall put in place adequate systems for documenting their principal activities and ensuring that they create and maintain records that serve departmental functions and the standards detailed above.

The quality of the records must be sufficient to allow staff to carry out their work efficiently, demonstrate compliance with statutory and regulatory requirements, and ensure accountability and transparency expectations are met. The integrity of the information contained in records must be beyond doubt and be protected from unauthorised alteration or deletion.

Where appropriate, templates should be created and used, so that documents are produced consistently and quickly. In addition, version control procedures are required for the drafting and revision of documents and records.

### 7.2 Organisation and Classification of Records

All records should be organised and described in a uniform, logical manner so that they are easily accessible when required.

Classifying records and storing them in an appropriate structure enables the business to assign suitable retention periods and security controls.

Standardised referencing and titling should be employed, so that records can be easily identified and retrieved. Naming conventions will assist with using consistent terminology to improve efficiency. Titles given to digital and hard copy records and files should describe the content or subject matter accurately and helpfully.

NCG is making increasing use of the Microsoft 365 solution that enables more sophisticated labelling and governance functionality. Work is underway to develop technological policies to assist with classification, protection and appropriate destruction of records.

To reduce unnecessary duplication, documents should be stored in central folders that are accessible by relevant staff. Digital information should be filed in shared corporate workspaces wherever possible. Documents received via e-mail should be stored in these shared spaces and removed from mailboxes. File titles should be brief but comprehensible using a consistent format.

### 7.3 Security and access

All records must be stored with appropriate technical and administrative controls to prevent unauthorised access or disclosure of information. All records shall be stored in secure physical and electronic locations that reflect the nature, confidentiality and importance of the information within.

Records should not be available to only one person. They should be stored in centralised locations (for example office filing systems or shared network directories), with appropriate access control lists applied and managed. Duplication of documents should be strongly discouraged and kept to an absolute minimum. Where duplicates are unavoidable, they should be deleted as soon as possible with access reverting to only the single master copy.

Records that are vital to the continued functioning of NCG shall be identified and protected. All such critical data shall be protected by appropriate backup and disaster recovery policies.

Examples of critical data include:

- Financial records.
- Student records.
- Staff records.
- Records of Incorporation.
- Governance Minutes
- Statutory records.
- Insurance records.
- Health and Safety records.

### 7.4 Retention of Records

The most significant pieces of legislation regarding retention of records are the Data Protection Act 2018, the UK GDPR and the Freedom of Information Act 2000.

The FOI Code of Practice on the Management of Records states:

*‘As a general principle, records should be kept for as long as they are needed by the authority: for reference or accountability purposes, to comply with regulatory requirements or to protect legal and other rights and interests. Destruction at the end of this period ensures that office and server space are not used and costs are not incurred in maintaining records that are no longer required’.*

UK Data Protection legislation i.e. DPA 2018 and UK GDPR apply specifically to Personal Data and make it a legal requirement that such data is:

*'kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed'.*

NCG could be subject to enforcement action for failing to comply with the Data Protection legislation, including failing to demonstrate that it complies under the Accountability Principle. By having clear procedures for the retention and disposal of Records, NCG demonstrates its compliance with the legislation.

NCG's Records Retention Schedule is intended to:

- Provide a consistent approach and guidance regarding appropriate retention periods for different categories of Record.
- Ensure that key documents can be retrieved when needed.
- Promote consistency and the retention of the minimum volume of records while accounting for requirements imposed by legislation and regulation.

Information Asset Owners shall agree retention periods for the records for which they are responsible and annually review those periods to determine if requirements have changed.

The Record Retention Schedule shall include:

- **Type of document** - a description of the type of document or asset.
- **Retention Period** - the period for which the document must be retained.
- **Requirement / Reason** - the legislation, regulation or other obligation that dictates the Retention Period.
- **Responsible Manager** - Information Asset Owner.

### 7.5 Appraisal of Records

At the end of a designated retention period, appropriate action should be taken against the Record. The action will be one of the following:

- **Dispose** – The record can be disposed of using an appropriate method. This may be 'delete' for electronic records, or standard disposal for non-confidential paper records. All confidential records, including those containing personal or financial information shall be disposed of by cross shredding where possible and through the confidential waste system in all cases. A record should be kept of the disposal. For large scale destruction or storage of hard copy records, staff should contact the Information Governance team.
- **Review** – Records marked for review at the end of their retention period may be required for a longer period. Therefore, their status should be checked before any action is taken.
- **Anonymise** – Where appropriate, some records may be valuable for research purposes. Such records can be considered for anonymisation



meaning all personal data is removed or rendered permanently irretrievable.

### 7.6 Records of Disposal

For potentially significant information a record shall be kept of what has been disposed of, the reason for its disposal and who authorised its disposal. This requirement applies to both destruction and transfer to archive. This will ensure there is a transparent audit trail detailing evidence of records that have been destroyed in line with NCG's procedures.

Certificates or records of disposal shall be retained by management when information of potential significance is destroyed.

### 7.7 Destruction of Records

**Paper records** should be destroyed under confidential conditions. This may be incineration, pulping or shredding using a crosscut shredder. NCG employs an external, approved third-party to manage its confidential waste. All staff shall dispose of paper documents in the provided confidential waste bins.

**Electronic Records** should be destroyed based on the digital medium on which they reside.

## 8. Audit of Records / Information Asset Management

Good records management practice requires that an organisation undertake an audit of records management and systems. From this we can understand what records we hold, their location, and in what form they are held. It also allows us to evaluate our record keeping systems and implement any identified improvements.

To that end, the business shall complete an annual survey or audit of its records. While individual records need not be catalogued into a central Information Asset Register, the types and series of records held in each business area must be recorded and linked to the relevant Information Asset Owner.

The register shall also record the location and security measures in place to control the asset and the retention period to which the asset is subject.

## 9. Off-site storage and scanning

Any college or service considering offsite storage should consult the IG Team prior to engaging with any provider.





**10. Monitoring and Compliance**

Ongoing and monitoring of compliance with this policy will be carried out on a regular basis by the Information Asset Owners and the Information Governance team.

**11. Policy Review**

This policy shall be reviewed annually, or in the event of significant change.