POLICY / PROCEDURE TITLE		DATE OF APPROVAL
Information Security Policy		February 2024
APPROVED BY	**VERSION NO.**	**VALID UNTIL**
Executive Board	1.5	February 2025

OWNER	Director IDS
GROUP EXECUTIVE LEAD	Chief Information, Data & Estates Officer (CIDEO)
DOCUMENT TYPE	Policy ☒ Group Procedure ☐ Local Procedure ☐
PURPOSE	The purpose of this policy is to describe the management and security of NCG's information assets.
APPLICABLE TO	This Policy applies to: • Everyone who accesses NCG information assets or systems including but not limited to NCG staff, students, contractors and third parties. • All technologies or services used to access or process NCG information assets. • Information assets stored by NCG or by an external service provider on behalf of NCG. • Information transferred to or from NCG's systems.
EQUALITY ANALYSIS COMPLETED [POLICIES ONLY]	Yes ☒ No ☐ N/A ☐ (If EA not applicable, please explain)
KEY THINGS TO KNOW ABOUT THIS POLICY	1. This policy is concerned with the **management and security** of NCG's information assets. 2. The Information Security Policy sets out NCG's approach to information security management. It is in place to support NCG's strategic vision and to protect the confidentiality, integrity, and availability of the business's information assets and technology services. 3. This Policy applies to everyone who accesses NCG information assets or systems including but not limited to NCG staff, students, contractors, and third parties.
EXPECTED OUTCOME	Readers are expected to understand the organisational position on [insert as relevant], know their responsibilities in relation to the policy and comply with the terms of the policy.

MISCELLANEOUS	
LINKED DOCUMENTS	• Acceptable Use Policy • Access Control Policy • Policy Against Malicious Code
KEYWORDS	• Information Security • Information Assets • Information Governance

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?	An information security policy is required to ensure that an organisation's information assets are protected from unauthorised access, modification, or destruction. The policy provides a framework for protecting information assets and ensures that the organization is working in accordance with industry standards and regulations. It also establishes a set of guidelines for employees to follow with regard to the security of company information and IT systems. The policy helps to maintain the confidentiality, integrity, and availability of information assets and technology services.		

1. GENERAL POLICY STATEMENT

This policy is concerned with the management and security of NCG's information assets. An information asset is an item or body of information, an information storage system or an information processing system that is of value to the business. Information security is the practice of protecting the confidentiality, integrity and availability of information assets.

This overarching policy document provides an overview of information security and lists a set of policy documents that taken together comprise NCG's Information Security Policy.

2. POLICY PURPOSE

The Information Security Policy (the "Policy") sets out NCG's approach to information security management. The Policy, and the supporting Information Security sub-policies are in place to support NCG's strategic vision and to protect the confidentiality, integrity and availability of the business's information assets and technology services. In addition, such information and the way it may be processed is subject to UK legislation, in particular in accordance with the EU General Data Protection Regulations (EU2016/679) "GDPR" and the Data Protection Act 2018.

3. INFORMATION SECURITY OBJECTIVES

The objectives of this policy are to establish and maintain the confidentiality, integrity and availability of information, information systems, applications and networks owned or held by NCG by:

- Ensuring that information will be protected in line with all relevant legislation, in particular those relating to data protection, human rights and freedom of information.
- Ensuring that all members of staff are aware of their roles, responsibilities and accountability and fully comply with the relevant legislation as described in this and other Information Governance policies.
- Creating and maintaining within the organisation a level of awareness of the need for Information Security as an integral part of the day-to-day business.
- Supporting NCG's strategic vision through an approach that effectively balances usability and security.
- Protecting NCG's information assets, including 3rd party data assets being processed or held by NCG, and technology by identifying, managing and mitigating information security threats and risks.

- Identify, contain, remediate and investigate information security incidents to maintain and assist in improving NCG's information security posture.
- Ensure that the organisation can continue its commercial activities in the event of significant Information Security incidents.
- Maintain the ISMS in line with the requirements of the ISO27001 Standard

4. POLICY STATEMENT

NCG is committed to protecting its information appropriately and shall ensure that:

- It processes information in compliance with all applicable legislation, regulation and contractual obligations.
- It assigns both general and specific responsibilities for information security to defined roles.
- Deviations & exceptions from this Policy shall be investigated and addressed.
- Information assets shall be identified, classified and protected in accordance with this Policy and its sub-policies. Security controls shall be proportionate to the defined classification.
- All information processes, technologies, services and facilities shall be protected by information security controls as detailed in the sub-policies.
- During the onboarding process, all 3rd parties are required to complete the NCG Cyber Assurance Questionnaire before any procurement activities take place.
- Information security incidents shall be identified, contained, remediated, investigated and reported in accordance with the Information Security Incident Reporting Policy
- Back-up and disaster recovery plans shall be place in accordance with the Business Continuity Plan to mitigate risk of loss or destruction of information and/or services and to ensure that processes are in place to maintain availability of data and services.
- Data Loss Prevention policies are applied to all users and data across M365 and Multi Factor Authentication is a requirement for accessing NCG VPN services.
- All staff shall complete the Information Security Mandatory Training periodically.
- This Policy and the ISMS, shall be subject to a process of continual improvement including annual review.

5. LEGISLATIVE & REGULATORY FRAMEWORK

Supply and use of NCG IT facilities is bound by English law. The legal and regulatory framework is outlined below and includes but is not limited to:

- Data Protection Act 2018
- UK General Data Protection Regulations
- The Computer Misuse Act
- Equality Act 2010
- Official Secrets Acts
- The Criminal Justice and Public Order Act
- Obscene Publications Act 1959
- Laws of Defamation
- Telecommunications Act 1984 & Communications Act 2003
- The Copyright Designs and Patents Act 1988
- International Law

Related guidance and codes of best practice include:

- ISO 27001:2013

6. ROLES & RESPONSIBILITIES

Role	Responsibilities
Chief Executive Officer	• Responsible for the implementation of this policy across the organisation
Executive Directors	• Implementing this policy on behalf of the CEO by ensuring their staff are fully aware of this policy and the operating procedures • Encouraging a 'responsible' culture that encourages staff to protect NCG data assets
Chief Information Officer Data & Estates Officer	• Overall responsibility for Information Security • The development, review and evaluation of this Policy • Ensuring the ISMS conforms wherever possible to the ISO27001 Standard • Reporting on the performance of the ISMS
Director – Information Governance	• Ownership of this Policy, review and update in line with legislation, regulation and best practice • Ensure all Information Security Policies are reviewed, updated and improved periodically
Information Governance Team	• Internal audit • Investigation of Information Security Incidents
Data Protection Officer	• As a public authority NCG is required to appoint a Data Protection Officer by the GDPR. The DPO is responsible for providing advice, monitoring

	compliance, and is the first point of contact in the organisation for data protection matters.
Director of Information and Data Services	• Review of this Policy periodically and submission of revisions to Group Executive for approval as necessary
Human Resources	• Responsible for the management of any personnel or misconduct matters arising from noncompliance with this Policy
Line Managers	• Ensuring their staff understand and comply with the organisation's policies and procedures

User Types

NCG Information Services maintains the directory of people authorised to use NCG IT facilities. These are defined as staff, students, external users and guests as follows:

- Staff are those users registered on NCG Personnel/Payroll systems.
- Students are those users registered on NCG Learner Management Information Systems.
- External users are all other users permitted access to NCG IT systems via a domain account.
- Guests are users permitted temporary access to NCG public IT facilities.

All users are subject to the NCG Acceptable Use Policy but have differing rights and responsibilities.

All Staff

All staff (including agency and contract staff) shall agree to written terms and conditions covering use of IT when they register to use NCG IT systems. HR / Information Services shall ensure that:

- Temporary staff accounts will be set to expire at the end of the staff contract period.
- Confidentiality agreements form part of the terms and conditions of employment.
- Awareness training about electronic information security forms part of NCG staff induction programmes.
- All references are checked by People Services prior to a member of staff's commencement of employment.

Schools and Services must ensure that where there are specific security roles and responsibilities that these are documented in all relevant job descriptions and that there is appropriate screening of applicants. Access to NCG systems may be withdrawn and NCG disciplinary procedures shall be invoked where a serious or deliberate breach of the policy is made.

Students

To use NCG IT, students shall agree to NCG terms and conditions contained within NCG learner agreement and abide by NCG Acceptable Use Policy. NCG disciplinary procedures, including withdrawal of access to systems, may be invoked if students fail to carry out their responsibilities under this policy.

External Users

Due to Microsoft Licensing and Cyber Insurance Policy, all 3rd party access has been removed as of November 2021.

Examples of external users are:

- People teaching on college courses who are not employed by the NCG.
- External examiners
- Outside researchers collaborating with NCG researchers
- Auditors
- Consultants
- Governors

External users are allowed access to NCG Guest Wi-Fi by means of employee sponsorship, approval and authentication. Any breach of the NCG Acceptable Use Policy may result in suspension of the account as well as possible disciplinary/legal proceedings against the user and or sponsor.

All external users of NCG IT systems and services must read and agree to NCG Acceptable Use Policy.

Guests

Guest user accounts and open access facilities may be used to allow visitors strictly limited access to public NCG IT systems e.g. NCG Guest Wireless. Digital records of such IT use (who, when and where) are held within the system.

Access to corporate systems, protected electronic resources, NCG e-mail services and personal file store will not be permitted for guest users.

7. LEGISLATIVE & REGULATORY FRAMEWORK

NCG’s Information Security Management System comprises this Policy and a suite of sub-policies.

Policy	ISO 27001 Reference
Access Control Policy	A 9.1.1
Policy Against Malicious Code	A 12.2.1
Portable IT Equipment Policy	A 6.2.1
User Access Management Procedure	A 9.2

8. PHYSICAL & ENVIRONMENTAL SECURITY - ACCESS

Access to NCG IDS systems; NCG Data Centre housed in Rutherford building, Newcastle College, subsidiary server rooms and rooms containing data communications or telephone equipment must be both controlled and restricted. Authority to access these areas will be controlled by the NCG Director IDS and NCG Head of Infrastructure (or nominated assistant) and administered by NCG Estates. Records of authorisation will be maintained by NCG IDS. Access control will be by various means including smart card, key lock, digital lock or biometric as appropriate. Communications equipment will normally be located in dedicated rooms that should not be used for any other purpose.

Equipment Security

Servers holding corporate information will be held in a secure environment protected by:

- Physical security and access control
- Fire detection and extinguishing systems
- Temperature and humidity control
- Water sensors
- Stable, conditioned electrical supply protected by uninterruptible power supply (UPS) and standby generator
- NCG electronic information will be held on servers approved by NCG IDS. External hosting must not take place without prior approval from the NCG Director IDS.

NCG Infrastructure Manager must ensure that IT Infrastructure is covered by appropriate hardware and software maintenance and support.

Clients must be appropriately secured and operated by NCG staff who must be trained in and fully conversant with this policy and their personal responsibilities for confidentiality of information displayed on the screen or in printed output. Backup media must be retained in accordance with NCG policy on retention of records and the Data Protection Act 2018.

All NCG data must be cleared securely from NCG IT equipment and media on disposal (in strict accordance with NCG Secure Disposal of Electronic Media procedures).

9. COMMUNICATIONS AND OPERATIONS MANGEMENT – REPORTING & INVESTIGATING SECURITY INCIDENTS

- Staff, students and employees should report suspected security breaches through their line manager to the Group Service Desk. The Service Desk system will be used to record suspected information and data security incidents. These incidents will be monitored by the NCG Information Security Lead and an appropriate investigation and action plan will be prepared. Details of incident reporting procedures can be found with NCG Incident Reporting Policy located on NCG intranet.
- Within the provisions of the law, NCG reserves the right at any time to intercept and monitor communications in accordance with the Regulation of Investigatory Powers Act; The Telecommunications (Lawful Business Practice), (Interception of Communications) Regulations and any other relevant legislation. Monitoring and recording is carried out routinely as part of systems operation and auditing. Specific interception/monitoring of individual activity shall normally only take place with the express approval of the NCG Chief Information, Data & Estates Officer.

OPERATIONAL PROCEDURES & RESPONSIBILTIES FOR INFORMATION SYSTEMS

NCG IDS will maintain written procedures for the operation (e.g. start up, backup, shut down and change control) of those NCG Business Systems where risk and impact would be high if such procedures were not carried out correctly. Performance of these systems will be monitored to ensure reliability.

10. PROTECTION AGAINST MALICIOUS SOFTWARE & HACKING

- All systems will be protected by a multi-level approach involving NGFW firewalls, router configuration, e-mail scanning, EDR with spy/malware protection on all clients within the NCG network. All NCG clients will have appropriate EDR software installed by NCG IDS configured to update anti-virus signatures automatically.
- Staff and students may use their own PC hardware to connect to the wireless network where a guest network is available. Only equipment owned by NCG may be connected to the NCG network. All hosts used by the employee or learner/customer that are connected to the NCG Internet/Intranet/Guest, whether owned by the employee or

NCG, shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.

- Network traffic will be monitored for unusual activity via managed SIEM Service/PRTG Sensors. This also includes daily web filter keyword searches in line with prevent duty and safeguarding. Keyword list is held centrally by NCG IDS and is provided by NCG Executive Director Quality. Regular vulnerability testing (internal/external) is held quarterly.

11. HOUSEKEEPING

- System backups will be performed by the relevant IDS support staff in accordance with documented procedures. The procedure will include keeping backups off site in secure storage. Periodic checks will be made to ensure backup media can be read and files restored. Records of backups will be monitored by IDS managers and be subject to random audit by internal and external auditors.
- Backups of corporate data are taken on a daily basis for critical systems or less frequently if appropriate. Backups protect electronic information from major loss or failure of system software and hardware. Backups are not designed to guard against accidental deletion or overwriting of individual user data files, backup and recovery of individual user files is the responsibility of the owner.

12. MANAGEMENT OF NETWORK CONFIGURATION AND SECURITY

- The configuration of critical routers, firewall and other network security devices will be the responsibility of, maintained by, documented and kept securely by the NCG Security Lead.
- No IT equipment may be connected to the network without approval by the NCG Security Lead. NCG IDS Security will disconnect and remove equipment that has not been approved.

13. EXCHANGES OF INFORMATION WITH EXTERNAL ORGANISATIONS

- Requests by external bodies for the provision of electronic information from Business systems will be referred to the system owner. This includes Data Subject Access Requests made under the auspices of the Data Protection Act 2018.

- Responses to Data Subject Access Requests in respect of systems owned and operated by NCG IT Services will be coordinated by the NCG IDS on request from NCG Governance. Requests for information under the Freedom of Information Act will be referred to the Clerk to the Corporation. All electronic information will be handled in accordance with NCG Data Classification Policy.

14. INTERNET & EMAIL

Use of e-mail and Internet is governed by the Acceptable Use Policy.

15. SOFTWARE INSTALLATION

All software installations on NCG systems must be in accordance with NCG procedures and copyright legislation. All software installed or introduced to NCG systems must be via the Software Request procedure located on NCG Intranet.

16. ACCESS CONTROL - ACCESS CATEGORIES

Access to IT will be restricted according to the type of user. NCG staff, students and external users may use:

- Standard software portfolio via System Centre Apps
- Shared file store**
- M365
- NCG Business systems**
- Electronic learning resources
- Internet
- Intranet**

**These services will not be provided to external users (e.g. representatives of external organisations with their own email accounts).

Guest users may use:

- Standard software portfolio
- Limited electronic learning resources where permitted by licence agreement
- Internet

17. USERNAME AND PASSWORD CONTROL

Primary access to all NCG IT is governed by a network username and password granting access to a set of network services as defined within the NCG policies. NCG IDS maintain procedures for the issue of and closure of network accounts. Authorisation of access to Business systems and to the data held by them is the responsibility of the system owner.

The control of network passwords is the responsibility of NCG DS. The resetting of network passwords is via NCG Service Desk and M365 Azure Self-Service following a documented procedure.

NCG IDS maintains records of the issue of system administrator passwords and ensures they are stored securely. System administrator passwords will be issued on the express authority of the NCG Director IDS on a need-to-know basis. Such passwords will be changed annually and when authorised system administrator staff leave the organisation.

For Windows operating systems the following will be enforced:

- network passwords must be a minimum of 12 characters with complexity
- network passwords will be subject to enforced periodic change
- network password history will prevent reuse of the last
- All Staff and Students accounts require MFA
- Conditional Access is active for all NCG accounts based on High Risk signins
- Accounts will be locked on the third failed login attempt

Policy on network password complexity is reviewed annually.

NCG IDS must be notified when staff leave and will be responsible for removing their network accounts. This is currently via staff leavers list presented by HRMIS. Responsibility for retention of any files held by staff who leave lies with their school/service and should form part of their staff exit procedure. Guidance is provided for M365 Cloud storage and scales of access. Schools and Services responsible for electronic information assets will be informed when staff authorised to access those assets leave and will be responsible for controlling/requesting access rights to those assets.

18. MOBILE COMPUTING

The danger to information stored on portable computers (laptops, notebooks, tablets and smart phones) is recognized and NCG resources are to be used in strict accordance with the NCG Acceptable Use Policy. Wireless computer networks potentially introduce new security risks and should be used in accordance with NCG Acceptable Use Policy. All mobile devices are encrypted with Bit locker encryption. Mac devices are encrypted via File Vault.

19. AUDITING & MONITORING

All use of NCG IDS systems may be monitored and audited in accordance with the Policies on using NCG IDS Resources. Remote access by third party contractors to maintain and support NCG IT systems is currently prohibited.

20. BUSINESS CONTINUITY PLANNING

The NCG Business Continuity Plan is contained within NCG Intranet.

21. STATEMENT ON POLICY IMPLEMENTATION

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

22. 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. Any issues highlighted in the assessment have been considered and incorporated into the policy and approved by the Lead Director and relevant committee.

23. STATEMENT ON CONSULTATION

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

VERSION CONTROL				
Version No.	**Documentation Section/Page No.**	**Description of Change and Rationale**	**Author/Reviewer**	**Date Revised**
1.0		Annual Review	N/A	May 2015
1.1		Annual Review & update to reflect new IT dept. structure.	N/A	Aug 2016
1.2		Annual Review	N/A	August 2017
1.3		Review and update for new legislation.	N/A	May 2018
1.4		Annual Review	N/A	June 2019
1.5		Updated to new NCG Policy Format	Director IDS	January 2024