POLICY / PROCEDURE TITLE		DATE OF APPROVAL
Data Protection Policy		July 2024
APPROVED BY	**VERSION NO.**	**VALID UNTIL**
Corporation Board	7	July 2027

OWNER	Director of Assurance & Risk		
GROUP EXECUTIVE LEAD	Chief Finance Officer		
DOCUMENT TYPE	Policy ☒	Group Procedure ☐	Local Procedure ☐
PURPOSE	The purpose of this policy is to set the standards for processing data and responding to data subject rights requests as required by relevant legislation such as the Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulation (GDPR)		
APPLICABLE TO	This policy applies to personal data recorded in any medium, about any person including but not limited to, employees, consultants, vendors, agency workers, contractors, service users, governors, trainees/students, volunteers and/or any other parties who have a business relationship with NCG. This policy also applies to any rights requests exercised by the data subject in any format, in accordance with Articles 15 to 22 of the UK GDPR.		
EQUALITY ANALYSIS COMPLETED [POLICIES ONLY]	Yes ☒	No ☐	N/A ☐
	(If EA not applicable, please explain)		
KEY THINGS TO KNOW ABOUT THIS POLICY	1. The UK GDPR applies to the processing of personal data that is wholly or partly by automated means or the processing other than by automated means of personal data which forms part of, or is intended to form part of, a filing system. 2. This policy is designed to comply with relevant legislation including the Data Protection Act 2018 and the UK General Data Protection Regulation GDPR.		
EXPECTED OUTCOME	Readers are expected to understand the organisational position on data protection, including knowing their responsibilities in relation to this policy and how to comply with the terms of this policy.		

MISCELLANEOUS	
LINKED DOCUMENTS	• Freedom Of Information (FOI) And Environmental Information Regulations (EIR) Policy • Information Policy • Information Governance Policy • NCG Special Category Data and Criminal Convictions Data Policy • Learner Privacy Notice • Staff Privacy Notice • Business to Business Privacy Notice
KEYWORDS	• Data Protection Act 2018 • UK GDPR

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 policy has been reviewed by the NCG Corporation Board.		

DATA PROTECTION DEFINITIONS

Data Protection Legislation	Data Protection Act 2018 (DPA 2018) United Kingdom General Data Protection Regulation (GDPR)
Personal Data	Any information in relation to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Data Subject	The identified or identifiable natural living person to whom the personal data relates to.
Data Controller	The natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Special Categories of Personal Data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
Criminal Convictions and Offences Data	Personal data relating to criminal convictions and offences or related security measures.
Consent	Consent of the data subject means any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which the data subject gives a statement or clear affirmative action, which signifies agreement to the processing of personal data relating to them.
Third Party	A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.
Employees	All current, former and prospective members of staff.
Students	All current, former, and prospective educational programme participants.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

Official Information	Information that relates to the organisation and its activities.
Supervisory Authority	An individual authority established by its member state to supervise the compliance with a specific regulation. The supervisory authority for the UK (and NCG) is the Information Commissioner's Office (ICO).
Privacy and Electronic Communications Regulations (PECR)	The Privacy and Electronic Communications (EC Directive) Regulations 2003.

1. INTRODUCTION

This policy:

- Is designed to ensure that NCG complies with the Data Protection Act 2018, the UK General Data Protection Regulation (GDPR) and the Common Law Duty of Confidence.
- Applies to all staff, trainees/students, agency workers, consultants, volunteers, governors, associates, partners, sub-contractors, customers, service users, and any and/or any other parties who have a business relationship with NCG.
- Provides guidance on processing personal data in compliance with the data protection legislation and with respect for confidentiality.
- Underpins and supports the Information Governance (IG) Framework where that applies to personal data.
- Requires staff to ensure that the organisation's Data Protection Officer (DPO) is consulted with before any significant new data collection or processing activity is initiated, to ensure that relevant compliance steps are addressed.

NCG is a registered data controller with the Information Commissioner's Office (ICO) with the registration number Z6977454. This means that NCG are responsible for how we hold and use personal data in line with the data protection legislation.

2. THE LEGISLATION

The UK GDPR is a UK regulation on data protection and privacy that sets guidelines for the collection and processing of personal information. When the UK left the European Union (EU) in 2020, the EU-GDPR was amended and written into UK law as the UK GDPR.

The Data Protection Act 2018 sets out the data protection framework in the UK and should be read in conjunction with the UK GDPR. It updates and replaces the previous legislation and came into effect on 25th May 2018.

The Privacy and Electronic Communications Regulations (PECR) sit alongside the Data Protection Act and the UK GDPR. They give people specific privacy rights in relation to electronic communications.

Data protection legislation exists to ensure that organisations are handling personal data legally and fairly for legitimate business purposes; to protect the rights and freedoms of individuals through the correct handling of personal data.

3. COMMON LAW DUTY OF CONFIDENCE

The common law of confidentiality is a broad principle of law that prevents a person who receives information from another party in confidence from taking advantage of it. That person must not make use of it to the prejudice of the person who gave the information without obtaining their consent.

A duty of confidence arises when one person discloses information to another (for example employee to employer) in circumstances where it is reasonable to expect that the information will be held in confidence. It is a legal obligation derived from case law and included in professional codes of conduct. When an individual has died, information relating to that individual remains confidential under the common law.

Confidential information is not confined to personal data, which is the only remit of the Data Protection Legislation. For example, commercial contracts are usually confidential as are exam papers (at least until the exams have been taken). NCG also implements Non-Disclosure Agreements, Data Processing Agreements and Data Sharing Agreements to this end.

4. ROLES AND RESPONSIBILITIES

NCG as Data Controller has a corporate responsibility to process personal data with due regard to the rights and freedoms of individuals, and to comply with the requirements of data protection law.

Data Protection Officer (DPO) and supporting team

All public bodies are required to appoint a DPO. It is the role of the DPO to assist NCG in monitoring internal compliance, inform and advise on data protection obligations and act as a contact point for data subjects and the ICO.

The DPO also helps demonstrate compliance in accordance with the enhanced focus on accountability. The responsibilities of the DPO must be formally documented when appointments are made, and they must be adequately trained to fulfil the role. For NCG, the DPO is the Director of Assurance and Risk.

The Data Protection Team has responsibility for providing advice on information governance issues, including data protection for processing, and recording requests for access to personal data and other rights existing under data protection law, for managing relevant complaints, for raising internal and external awareness of NCG's obligations, which includes training, and for notifying the Information Commissioner of the details of the DPO along with payment of the annual fee.

Principals and Professional Service Leaders

Principals and Professional Service Leaders must ensure that the activities and processes within colleges or departments (as applicable) are compliant with this policy, and that staff have a sufficient awareness and knowledge of relevant requirements and that appropriate processes are in place to ensure compliance.

Employees

All Employees are under legal and contractual obligations to keep personal and other information confidential not only during their employment (or equivalent) but also after employment has been terminated.

All Employees are required to complete mandatory Information Security and Data Protection training at the start of employment and every three years thereafter.

5. DATA PROTECTION PRINCIPLES

NCG will process personal data in accordance with the data protection legislation and adhere to the data protection principles as set out in the UK GDPR.

Data Protection Principles	How NCG Complies
Lawful, Fairness and Transparency	NCG issues privacy notices to its staff, students, and business contacts explaining how it processes and captures data and for which lawful purposes this processing applies. NCG's privacy notices are available on NCG's website.
Purpose Limitation	NCG will only use personal data for the purposes for which it was collected.
Data Minimisation	NCG will only collect personal data relevant to the purpose for which it is required.
Accuracy	NCG will ensure the data it processes is correct, up to date and able to be rectified promptly.
Storage Limitation	NCG will not store data for longer than it is required.
Integrity and Confidentiality (security)	NCG implements various measures to protect personal data from unauthorised access, loss or destruction. NCG's Information Security Policy describes the management and security of NCG's information assets. The policy is available on NCG's website.
Accountability	NCG will demonstrate its accountability by maintaining meticulous documentation of its data security and data handling measures; capturing details relating to rights requests and ensuring that data is stored and confidentially destroyed in line with the NCG Retention Schedule.

All employees are responsible for ensuring that the data protection principles are always adhered to and at all stages of the lifecycle of the data including:

- The collection or capture of personal data.
- The post collection processing of data e.g. storing, alteration, transmission etc.
- The erasure or destruction of personal data.

NCG is required by law to be able to demonstrate compliance with the Data Protection Principles. This is known as the Accountability Principle.

To support users in complying with the data protection principles when collecting personal data, a useful checklist is provided in **Appendix 1**.

6. RECORDS OF PROCESSING ACTIVITIES

Article 30 of the UK GDPR requires organisations to document all processing. This helps organisations to demonstrate compliance with the data protection legislation. This is recorded in a data-mapping document and these records are managed by the Data Protection Team.

7. LAWFUL BASIS FOR PROCESSING PERSONAL DATA

To process personal data lawfully, we must have a valid lawful basis to process personal data. A lawful basis must first be established before processing begins.

The six lawful bases are:

Lawful Basis	Explanation
Consent	The data subject has given consent to the processing of his or her data for one or more specific purposes. Where consent is relied upon to lawfully process Personal Data, the consent must be specific, informed and freely given. NCG will only obtain consent from a positive opt-in statement, consent will not be gathered on an opt-out basis (for example, pre-checked boxes). NCG will clearly inform data subjects how they can withdraw their consent.
Contract	The processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
Legal Obligation	The processing is necessary for compliance with a legal obligation to which NCG is subject.
Vital Interest	The processing is necessary to protect the vital interests of the data subject or of another natural person. For example, to protect an individual's life.
Public Interest	The processing is necessary for NCG to perform a task in the public interest or for official functions and the task or function has a clear basis in law.

Legitimate Interest	The processing is necessary for the purpose of legitimate interests of NCG or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, which require protection of personal data.

To process special category data, NCG is required to have:

- An additional legal basis for processing under Article 9.
- A specific policy document in place regarding handling Special Category data.

The NCG Special Category and Criminal Convictions Data Policy explains our obligations to process special category data, this policy can be made available upon request and is also available on our website here.

8. DECIDING ON THE APPROPRIATE CONDITION FOR PROCESSING

When assessing which lawful basis applies for processing data, we must first establish if the processing is necessary. This means the processing must be a targeted, appropriate way of achieving the stated purpose. We cannot rely on a lawful basis if we can reasonably achieve the same purpose by some other means.

Remember that more than one basis may apply, and we should rely on what will best fit the purpose, not what is easiest.

The Data Protection Team should be contacted where appropriate for advice regarding the lawful basis for processing personal data in your area of responsibility. The organisation's Data Protection Team can be contacted at DPO@ncgrp.co.uk.

9. RIGHTS OF THE DATA SUBJECT

The UK GDPR ensures that individuals have rights regarding the way that organisations handle personal data and NCG must ensure that all procedures that involve the processing of personal data can demonstrate how individuals can exercise these rights.

The rights of the data subject:

Rights	Explanation
Right of Access	Individuals have the right to access and receive a copy of their personal data, and other supplementary information. This is commonly referred to as a subject access request or 'SAR'.
Right to Rectification	Individuals have the right to have their personal data rectified if it is inaccurate or incomplete.
Right to Erasure	Individuals have the right to have their personal data erased. This is also known as the 'right to be forgotten'. Please note this right is not absolute and only applies in certain circumstances.
Right to Restrict Processing	Individuals have the right to request the restriction or suppression of their personal data. When processing is restricted, NCG is permitted to store the personal data, but not use it. Please note this is not an absolute right and only applies in certain circumstances.
Right to be Informed	Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the UK GDPR. NCG provides Privacy Notices to comply with this right.
Right to Data Portability	The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows individuals to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability. Individuals have the right to transmit those data to another controller without hindrance from NCG to which the personal data have been provided. This right only applies to information an individual has provided to NCG in a structured, commonly used and machine-readable format.
Right to Object	Individuals have the right to object to the processing of their personal data in certain circumstances. Individuals have an absolute right to stop their data being used for direct marketing. When this right is exercised, NCG will no longer process the personal data unless the NCG demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.
Rights in relation to Automated Decision Making and Profiling	Automated individual decision making is making a decision solely by automated means without any human involvement.

	Profiling is any form of automated processing of personal data to evaluate certain things about an individual. Profiling can be part of an automated decision-making process. NCG can only carry out this kind of decision making where the decision is: • necessary for the entry into or performance of a contract; or • authorised by domestic law applicable to the controller; or • based on the individual's explicit consent. To process data in this manner, NCG will ensure that: • individuals receive information about the processing; • we introduce simple ways for individuals to request human intervention or challenge a decision; and • regular checks are carried out to make sure that systems are working as intended.

Individuals can request to exercise these rights verbally or in writing. The NCG Data Subject Rights Request Form is available in **Appendix 2** of this policy for this purpose.

When a request to exercise any of the following rights is received by a member of staff, they must inform the Data Protection Team immediately.

10. PRIVACY STATEMENTS

Personal data must be processed 'in a transparent manner'. This is achieved by providing the data subject with information at the point of data capture, or if this is not possible, within a reasonable period after obtaining the data, but at least within one month. This information is known as a Privacy Statement, Privacy Notice or Privacy Policy.

NCG's Privacy Notices will comply with the Regulation and follow the relevant ICO guidance including but not limited to:

- At the point of capturing an individual's data, NCG will notify them of the ways in which their personal data may be held and processed.

- Where NCG relies on the consent of the data subject and a record of this consent must be maintained; in the case of special categories of personal data such consent must be explicit.
- Where the processing is for marketing purposes, the notification will highlight any opportunities to opt out of such communication. See Privacy Electronic Communications Regulations below for more information on marketing.
- If staff collect information about students, business contacts or others, they must comply with the guidelines set out in these procedures and the data collated should not exceed the general information needs.
- NCG will notify new employees and governors that their personal data will be processed for employment purposes prior to the employment contract being signed.
- Learners will be notified about the processing of their personal data and any opt-outs prior to signing their Learning Agreement, Enrolment Form or alternative document specified in the relevant contract.

Special category data can only be collected and processed if the appropriate legal conditions are met. Staff needing to collect special category information must ensure they have authorisation by the Data Protection Officer to do so. The only exception is if a non-authorised member of staff is satisfied that the processing of the data is necessary in the vital interests of the data subject. This exception is only applicable in limited circumstances such as medical emergencies.

The standard form for recording explicit consent is in **Appendix 3**.

The standard form for recording consent for images to be stored in media libraries and included in publications and publicity materials is in **Appendix 4**.

Forms completed to record consent will be sent to DPO@ncgrp.co.uk for storage and retention.

11. PRIVACY AND ELECTRONIC COMMUNICATIONS REGULATIONS

The Privacy and Electronic Communications Regulations places further obligations on NCG when sending out electronic marketing communications. The

recipients of electronic marketing communications are broken down into the following categories:

- Individual Consumers (including sole traders) i.e. personal contact details such as telephone number, e-mail address, home address etc.
- Corporate Subscribers (business to business) i.e. an individual's work e-mail address, work telephone number, work address etc.

To send direct marketing to an Individual Consumer, NCG **must** be able to demonstrate evidence that the data subject has given their explicit consent to market to them. To send direct marketing to a Corporate Subscriber, there is no requirement to evidence consent as it is considered as a 'legitimate interest'.

When contacting both Individuals or Corporate Subscribers for marketing purposes, staff must always include a link to or a copy of a privacy notice in every communication, as well as give the recipient the opportunity to 'opt out' of receiving any future communications. In terms of e-mail communications, this can be done by adding in an 'Unsubscribe' link in the footer of any e-mails, or a statement advising that they can reply 'STOP' to unsubscribe. If an individual wishes to opt-out i.e. exercise their 'right to object' to direct marketing, this is their absolute right and therefore staff must ensure that no further marketing communications are sent to them.

When deciding if it is acceptable to send out electronic marketing communications, please refer to the direct marketing guidance provided by the ICO which can be accessed here.

12. PRIVACY BY DESIGN AND DEFAULT AND DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

NCG is required to ensure that it follows a procedure of Privacy by Design when processing personal data. This requires NCG to have the necessary technical and organisational measures to ensure that by default, only personal data which is necessary for any particular purpose is processed.

Where a type of processing (taking into account the nature, scope, context and purposes of the processing) is likely to result in a high risk to the rights and

freedoms of natural persons, NCG will, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A DPIA is required by the UK GDPR in the case of:

- When using new technologies.
- Systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person.
- Processing on a large scale of special categories of data and personal data relating to criminal convictions and offences.
- Systematic monitoring of a publicly accessible area on a large scale.

A DPIA helps identify and minimise the data protection risk of a project. It must contain the following:

- At least a general description of the processing operations and the purposes.
- An assessment of the risks to the rights and freedoms of individuals.
- The measures envisaged to address those risks.
- The safeguards, security measures and mechanisms in place to ensure you protect the personal data.
- A demonstration of how you are complying with Part 3 of the Act, taking into account the rights and legitimate interests of the data subjects and any other people concerned.

The responsibility for completing DPIAs lies with a member of staff, who has enough authority over a project to effect change, e.g. a project lead or manager.

Prior to conducting a DPIA, please contact the Data Protection Team at DPO@ncgrp.co.uk for guidance to confirm if a DPIA is required. The Data Protection Team will consult and guide colleagues when completing this and can be made aware of the high-risk data being processed.

13. DOCUMENT RETENTION

The UK GDPR does not dictate how long you should keep personal data however, the Storage Limitation principle states that *"data should be kept in a form which permits identification of a data subject for no longer than is necessary."* This means that the data must only be stored for as long as it is required. NCG will determine the suitable retention period for data being processed and ensure that once the data has reached this threshold, it is securely destroyed, anonymised or erased. The retention period of the data will be determined by the purpose for which it is processed and the lawful basis for processing it.

For data processed by NCG, the retention period and relevant justifications are recorded in the NCG Document Retention Schedule. This schedule can be accessed on the NCG website.

It is the responsibility of relevant management to ensure that both paper and electronic records are retained or disposed of accordingly, in line with the NCG Document Retention Schedule.

14. CRIMINAL OFFENCE DATA

Article 10 of UK GDPR sets out high-level conditions for the processing of personal data relating to criminal convictions and offences. DPA 2018 sets our specific conditions for such processing in Schedule 1. NCG will only process criminal offence data in accordance with the current data protection legislation.

The DPA 2018 requires that:

- When the processing is carried out, the controller has an appropriate policy document in place. To meet this requirement, NCG has established conditions for processing in the NCG Special Category and Criminal Convictions Data Policy.
- Organisations record the lawful condition for processing such data. This will be determined prior to any processing and will be recorded in the relevant data mapping document and/or DPIA.

NCG will not keep a comprehensive register of criminal convictions.

15. DATA PROTECTION BREACHES

A personal data breach is a security incident that has affected the confidentiality, integrity or availability of personal data. This includes incidents that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data. In short, there will be a personal data breach whenever any personal data is accidentally lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

Any breach of this policy or of data protection legislation, must be reported to the Data Protection Team at DPO@ncgrp.co.uk as soon as the breach has been discovered; this means as soon as you have become aware of a breach.

NCG has a legal obligation to report high-risk data breaches to the ICO within 72 hours and to record all other breaches, including minor breaches.

All members of staff have an obligation to report actual or potential confidentiality or data protection compliance failures. This allows NCG to:

- Establish whether a personal data breach has occurred.
- Investigate the failure and take remedial steps if necessary.
- Maintain a register of compliance failures.
- Establish the likelihood of the risk to people's rights and freedoms. If a risk is likely, we must notify the ICO without undue delay, but no later than 72 hours after becoming aware of the breach.

Any member of staff who fails to notify of a breach or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures could be subject to disciplinary action.

Please refer to the NCG Information Security Incident Reporting Policy for our reporting procedure which can be made available upon request from DPO@ncgrp.co.uk.

16. CONTRACTS AND DATA SHARING

Before sharing data with any other party, NCG will put in place suitable agreements that cover the data protection requirements for that sharing. These agreements will be one of the following:

- Data sharing agreement – is put in place where NCG are acting with another controller as joint controllers of personal data. There is a legal obligation to set out NCG's responsibilities in a joint control arrangement, under both the UK GDPR/Part 2 of the DPA 2018 and under Part 3 of the DPA 2018. The agreement details, but not limited to agreed roles and responsibilities for complying with the UK GDPR.
- Standard Contractual Clauses – contractual clauses under UK GDPR Article 28 that are required between a Data Controller and Data Processor.
- Data Processing Agreement – an agreement between NCG and individuals, similar to an NDA, but relating to Personal Data. This is to be used in the absence of a formal contract between companies for example, between NCG and a consultant who is authorised to access NCG systems containing Personal Data.

17. EDUCATION AND AWARENESS

All staff will complete the Information Security and Data Protection module during their mandatory training. This training must be repeated every three years.

18. POLICY UPDATES

This policy and its procedures will be updated without undue delay when they require changes, e.g. because of operational change, court or regulatory decisions or changes in regulatory guidance.

19. STATEMENT ON IMPLEMENTATION

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

20. 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.

21. STATEMENT ON CONSULTATION

This policy / procedure has been reviewed in consultation with the Policy Review Council and Executive Board prior to being approved by Corporation.

VERSION CONTROL				
Version No.	**Documentation Section/Page No.**	**Description of Change and Rationale**	**Author/Reviewer**	**Date Revised**
1	New Policy Developed	Reworking of previous documentation, updating to DPA 2018 compliance.	Director of Assurance & Risk	Feb 2019
2	Full Review	Review and minor updates to include references to Governors.	Director of Assurance & Risk	Feb 2020
3	Full Review	Annual review – inc. confidentiality clauses & simplification.	Director of Assurance & Risk	July 2020
4	Full Review	Updates to reflect the change in the legislation references after Britain left the European Union.	Director of Assurance & Risk	Jan 2021
5	Full Review	Annual review inc. Accountability Principle & Data Sharing arrangements.	Director of Assurance & Risk	June 2021
6	Full Review	Annual review – no material changes	Director of Assurance & Risk	June 2022 & 2023
7	Full Review	The policy has been reviewed to ensure it complies with the ICO guidelines. Minor amendments. Will change to 3-year review cycle.	Director of Assurance & Risk	June 2024

APPENDIX 1 – PERSONAL DATA PROCESSING CHECKLIST

This checklist should be used whenever there are plans to collect personal data for the first time or in respect of processing activities that are not already routinely carried out by NCG. If you have answered **no** to any of the below questions, contact the Data Protection Team at DPO@ncgrp.co.uk before proceeding.

Consideration	Yes / No / Not Required	Details / Justification
Is it necessary to collect this data?		
Have I checked there will be no unjustified adverse effects on data subjects as a result of this processing?		
Has the use of anonymised / pseudonymised data been considered instead?		
Has a privacy notice been provided to the data subject? (describe how)		
Is any potential further processing covered in the privacy notice?		
Has an Article 6 lawful basis been identified?		
Has an Article 9 lawful ground been identified (only if special category data)?		
Is the activity recorded in NCG's Record of Processing Activity?		
Have reasonable steps been taken to ensure the accuracy of the data?		
Will the data be processed securely?		

If the data will be shared with others, does the subject know to expect that?		
If a third party will process this data on NCG's behalf, is there a contract in place that has been approved by the NCG Legal and Contracts Team?		
Do you know how long to keep the data for?		
Have I checked that processing (taking into account the nature, scope, context and purposes) will **not** likely result in a high risk to the rights and freedoms of natural persons?		
Have I checked the processing does **not** involve the following: • Using new technologies. • Systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person. • Processing on a large scale of special categories of data and personal data relating to criminal convictions and offences. • Systematic monitoring of a publicly accessible area on a large scale.		

APPENDIX 2 – DATA SUBJECT RIGHTS REQUEST FORM

NCG Data Subject Rights Request Form

Please complete this form if you wish to exercise one or more of your rights regarding your personal data under the UK General Data Protection Regulations (GDPR).

Once you have completed this form, please submit this to us via DPO@ncgrp.co.uk. We will endeavour to respond promptly within one calendar month of receipt.

The information you supply in this form will only be used for the purposes of helping us to identify and collate the relevant personal data to respond to your request.

You do not have to use this form to ask for copies of your data, however, doing so will help us to know specifically what you are looking for to ensure that we can respond fully and promptly.

Section 1. Who is making the request?

We ask for your contact details so we can send your response and discuss your request with you (if needed). You only need to give us relevant details i.e. your postal address if you'd like a response sent by post. We may ask you for proof of ID if we feel it's reasonable and proportionate. The timescale for responding to your request will start when we receive this.

Full Name*	
Contact Number*	
Email Address*	
Postal Address (if applicable)	

Are you making this request on behalf of someone else?

☐ - Yes

☐ - No (Please move to section 3)

Section 2. Please provide the contact details for the person you are making the request on behalf of:

Name of Data Subject	
Contact Number	
Email Address	
Postal Address (if applicable)	

You will need to give us proof of your authority to act on their behalf e.g. this could be written authorisation from them or a relevant power of attorney.

Please send proof of authority together with this form when you make your request.

☐ - Yes, I've got proof of my authority to act on someone else's behalf and I'll include it with my form (Please move to section four).

☐ - No, I haven't got any proof of authority yet, but will provide this at a later date once obtained. I understand you can't action my request until you receive this information.

Section 3. How would you like us to respond to you?

☐ - Email

☐ - Post

☐ - Other (please specify)

_____

Section 4. Please place an 'X' the appropriate box to indicate which of your data subject rights you wish to express:

☐ - Right of Access (Subject Access Request)

☐ - Right to Data Portability

☐ - Right to Object

☐ - Right to Restrict Processing

☐ - Right to Erasure

☐ - Right to Rectification

Section 5: Details of your request:

Please provide as much detail as possible about your request to help us to identify the information you require.

To enable us to locate the relevant data which you require in a timely manner, please provide as much information as possible regarding:

- the type of data in question.
- the period during which the data has been held.
- the persons or departments who are likely to be holding this data.
- and the sites and/or specific locations where such persons or departments are based.

Please state below exactly what personal data you are looking for, for example, if you need a specific email, we could search for this using a particular word or phrase; the date range of the personal data you are asking for; a particular report and/or department file:

Please note that if the information you request reveals details directly or indirectly about another person, we will have to seek the consent of that person before we can disclose that information. In certain circumstances, where disclosure would adversely affect the rights and freedoms of others, we may not be able to disclose the information to you, in which case you will be informed promptly and given full reasons for that decision. There may be other relevant exemptions under the Data Protection Act 2018 that prevent NCG disclosing information to you. While in most cases we will be happy to provide you with copies of the information you request, we reserve the right in accordance with Article 12 of the UK GDPR to charge a fee or refuse the request if it is considered “manifestly unfounded or excessive”. However, we will make every effort to provide you with a satisfactory form of access or summary of information if suitable.

Section 6: (To be completed only for a Request for Data Portability)

Please tick the appropriate box to indicate the format that you would like us to use to transmit the requested data:

☐ - Microsoft Office (Word, Excel etc.)

☐ - OpenDocument

☐ - PDF

☐ - Other (Please Specify):

_____

Please note that it may not always be possible to transmit your data in your requested format, however we will notify you of this prior to sending.

Section 7: Are you the data subject?

To ensure we are communicating with the right person we require you to provide us with proof of your identity and of your address. Please supply us with a photocopy or scanned image (do not send the originals) of one or both of the following:

1) Proof of Identity (passport, photo driving licence, national identity card, birth certificate).

2) Proof of Address (utility bill, bank statement, credit card statement (no more than 3 months old); current driving licence; current TV licence; local authority tax bill, HMRC tax document (no more than 1-year-old).

If we are not satisfied you are who you claim to be, we reserve the right to refuse to grant your request.

Declaration

I, …….. certify that the information given on this application form to NCG is true. I understand that it is necessary for NCG to confirm my identity and it may be necessary to obtain more detailed information in order to locate the correct information.

Signed: ……**Date**: ……

Please return the completed form and accompanying items to DPO@ncgrp.co.uk or via post at NCG Data Protection Officer, NCG, Rye Hill Campus, Scotswood Road, Newcastle upon Tyne NE4 7SA

APPENDIX 3 – NCG CONSENT FORM

NCG Consent Form

Name:	
Student ID number/ Staff payroll number:	
Address:	
Contact number:	
E-mail address:	

Please select Consent to share or Refusal of consent to share below:

Consent to share
I hereby consent for my personal data including sensitive personal data to be: • processed by NCG • disclosed to the following third parties: [Please insert the name of third parties here] The personal data that will be shared with the above third parties: • [Please list all the personal data that will be shared here] for the following purposes:

A. [Please list the purpose of collecting and sharing the personal data including why the data is wanted and what NCG and the above third parties will do with the data] B. [Insert here] C. [Insert here] D. [Insert here]
☐ By ticking this box, **I consent** to information sharing.

Refusal of consent to share
☐ By ticking this box, **I do not consent** to the above information sharing.

I understand that I have the right to withdraw my consent at any time and can do so by contacting NCG's Data Protection Officer via dpo@ncgrp.co.uk.

Signed: ..... Date: .....

Once completed, please submit this form to the Data Protection Team DPO@ncgrp.co.uk.

APPENDIX 4 – APPROVAL FORM [PHOTOGRAPH, QUOTE, FILM]

Approval Form
(Photograph, Quote, Film)

If the participant is considered a 'vulnerable person', their involvement must be discussed in advance with the appropriate safeguarding lead.

Section A – to be completed at the outset by the participant

Name:

Address:

Telephone number:

E-mail:

Name of Course/Programme:

Year: 1 2 3

Are you an employee, student, business contact, parent/guardian or other? (Please state):

Quote (if relevant):

I confirm that NCG are permitted to use photographs, quotes and film footage of myself in ANY/ALL publicity material (The organisation comprises Newcastle College, Newcastle Sixth Form College, West Lancashire College, Kidderminster College, Carlisle College, Lewisham College and Southwark College). I understand that I have no interest in the copyright or any moral rights in any of the above and will not be contacted again for permission of usage. I understand that the choice of what is used is solely up to NCG and that when issued/printed it may be used as seen fit in prospectuses, press releases and other publicity materials. I understand that I have the right to withdraw my consent for the use of the material I have provided, however it is not possible for NCG to cease use of the material that is already printed or made publicly available prior to my withdrawal. If photos &/or quotes are sent to

the media, I understand that they may use these as and when they think it is appropriate and I understand that I have no interest in this. I am 16 years of age or over.

Signed: …… Date: ……..

Section B - for NCG internal use

Date of shoot/quote:

Location:

Description of model for identification:

Photographer/Operative/Marketing Department Representative:

Once completed, please submit this form to the Data Protection Team DPO@ncgrp.co.uk.