LTE Group
Data Protection Policy

LTE Group is the UK's first integrated education and skills group offering learning right across the spectrum. LTE group is the largest social enterprise of its kind. Retains charitable status and supports national and regional government aims.

For further details of LTE Group, please visit our website:

www.LTEgroup.co.uk

Date Approved:	**May 2018**
Approved by:	**LTE Group Board**
Review Date:	**May 2019**
Responsible Manager:	**Data Protection Officer**
Accessible to Staff:	**Yes**
Accessible to Students:	**Yes**
Relevant to TMC:	**Yes**
Relevant to UCEN MCR:	**Yes**
Relevant to Total People:	**Yes**
Relevant to MOL:	**Yes**
Relevant to Novus:	**Yes**
Relevant to Novus Cambria:	**Yes**

Document Purpose:

The purpose of this documents is to help you understand the scope of the General Data Protection Regulation (EU) 2016/679 ("**GDPR**") to enable LTE Group to comply with the law.

This policy therefore sets out the responsibilities of anyone who Processes Personal Data on behalf of the Group, including directors, full and part-time employees, workers and contractors. It includes information on:

(a) The scope of the data protection legislation

(b) The data protection principles

(c) Lawfulness, fairness, transparency of data processing

(d) Purpose limitation

(e) Data minimisation

(f) Accuracy

(g) Storage limitation

(h) Security, integrity and confidentiality

(i) Reporting a Personal Data Breach

(j) Transfer limitation

(k) Data Subject's rights and requests

(l) Accountability

(m) Direct marketing

(n) Definitions of key terms used in this policy

Reference or Associated Documents

Ref.	Document Title
ITS003	LTE Group IT Services Information Security Policy
ITS007	Encryption Policy
ITS011	LTE Group IT Services Access Control Policy;
ITS027	Clear Desk Policy
ITS039	Disposal and Re-Use of Media Policy
ITS042	Network Security Policy
ITS049	Information Data Retention Policy
ITS069	LTE Group IT Services Acceptable Use Policy
ITS070	Risk Assessment Methodology
ITS098	Password Policy
ITS099	Information Exchange Policy
ITS111	System Configuration Policy
ITS169	LTE Group Bring Your Own Device Policy

Table of Contents

1 Introduction

The way in which LTE Group, which includes Total People Limited (Work Based Learning and Novus Cambria- a joint venture with Coleg Cambria, and the operating divisions of the LTE Group (statutory corporation) – Novus (delivery learning and skills in the Prison estate), The Manchester College (FE delivery), UCEN (HE delivery), MOL (blended distance learning) and LTE Group Services – ("**we**", "**our**", "**us**", "**the Group**"), use personal data is regulated by data protection legislation. From 25 May 2018, this includes the General Data Protection Regulation (EU) 2016/679 – the "**GDPR**".

It is important for all our Colleagues ("**you**", "**your**") to understand the scope of the GDPR to enable us to comply with the law. This policy sets out the responsibilities of anyone who Processes Personal Data on behalf of the Group, including directors, full- and part-time employees, workers and contractors. Related Policies and are available to help you interpret and act in accordance with this policy.

The Information Commissioner's Office ("**ICO**") is the supervisory authority regulating data protection in the United Kingdom. Breaching the GDPR can lead to fines ordered by and payable to the ICO and/or claims for compensation. There is also a reputational risk of negative publicity for the Group. For these reasons, if you fail to comply with the requirements of this policy and the Related Policies, you may be subject to disciplinary action.

All Colleagues must familiarise themselves with this policy. Any questions or concerns about the interpretation or operation of this policy should be addressed to our Data Protection Officer at dpo@ltegroup.co.uk – in the first instance.

Some parts of the data protection legislation can sound quite technical and legal, particularly as a result of the various legal definitions and phrases that are used. We have therefore included a "Definitions of key terms used in this policy" section to this policy in paragraph 16. Any questions or concerns about the interpretation or operation of this policy should be addressed to the Data Protection Officer at dpo@ltegroup.co.uk in the first instance.

2 Scope of the data protection legislation

The GDPR applies to the "**Processing**" of "**Personal Data**" by automated means (electronically) or where Personal Data form, or are intended to form, part of a filing system.

We have explained below what this means in more detail below.

2.1 What is "Personal Data"?

Personal Data means any information about an individual from which that person (a "**Data Subject**") can be identified. It does not include data where the identity has been removed (anonymous data). The information will be Personal Data if a person can be identified either 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 person. For example personal data may include names, addresses, email addresses and telephone numbers; it may also include images in photographs or films and recorded telephone conversations.

We use Personal Data in relation to various types of Data Subject, including employees, learners, potential learners, business contacts, suppliers and contractors.

There are special categories of Personal Data to which additional safeguards apply. This means special category Personal Data needs to be treated even more carefully than Personal Data.

These special categories of Personal Data include information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation and biometric or genetic data. Personal Data relating to criminal offences and convictions has separate and specific safeguards to the special categories of Personal Data listed above. The Processing of Personal Data relating to criminal convictions and offences or related security measures shall be carried out only under the control of official authority or when Processing is authorised by (EU or Member State) law providing for appropriate safeguards for the rights and freedoms of data subjects.

2.2 What does "Processing" Personal Data mean?

The data protection legislation only applies to the "Processing" of Personal Data.

Processing has a broad definition and includes almost anything we might do with Personal Data, including obtaining, recording, organising, structuring, holding, using, disclosing and destroying Personal Data.

2.3 Who is the "Data Controller" and "Data Processor"?

A "**Data Controller**" determines the purposes for which and the manner in which Personal Data is processed. For example, your employer organisation within the Group is a Data Controller in respect of Personal Data it holds about you.

A "**Data Processor**" is any person who processes data on behalf of the Data Controller.

A Data Controller remains responsible for the use of any Personal Data that it passes to the Data Processor. We are also required to put in place a written contract with any Data Processors we use, to make sure that they reach the same high standards of data protection as LTE Group. Anyone wishing to appoint a Data Processor, or is concerned that they are passing Personal Data onto a third party (i.e. a person or entity outside of LTE Group) should speak to the Data Protection Officer to ensure that an appropriate contract is used.

While you are carrying out your role working for the Group, you will not be a Data Processor. However if you act outside of your contract or role, you may become a Data Controller or Data Processor, and the legal obligations that fall to the Group entities as Data Controller could equally apply to you. This is another reason it is really important for you to be aware of the importance of data protection.

If you have any concerns about this, please let the Data Protection Officer know.

3 The data protection principles

The data protection principles underpin the GDPR and tell us how we should Process Personal Data.

They are set out in the GDPR and require Personal Data to be:

a) Processed lawfully, fairly and in a transparent manner (*Lawfulness, Fairness and Transparency*).

b) Collected only for specified, explicit and legitimate purposes (*Purpose Limitation*).

c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (*Data Minimisation*).

d) Accurate and where necessary kept up to date (*Accuracy*).

e) Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (*Storage Limitation*).

f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (*Security, Integrity and Confidentiality*).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (*Accountability*).

We have explained these in more detail below as it is really important that you understand how these principles work in order to ensure our compliance with the data protection legislation and to make sure that you do not breach the data protection legislation.

4 Lawfulness, fairness, transparency

4.1 Lawfulness and fairness

Personal Data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

The GDPR only allows Processing for specific purposes. These are known as the lawful grounds of processing or the conditions of processing. You need to comply with one of these grounds to make the Processing lawful and in compliance with the data protection legislation. The most relevant are set out below:

a) the Data Subject has given his or her Consent; or

b) the Processing is necessary for the performance of a contract with the Data Subject; or

c) to meet our legal compliance obligations; or

d) to protect the Data Subject's vital interests;

e) to provide education (performing a task in the public interest); or

f) if the Processing does not relate to tasks carried out to provide education (our public task), to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we Process Personal Data for legitimate interests need to be set out in applicable Privacy Notices.

We have to identify at least one of the above legal grounds and document which one(s) we are relying on for each Processing activity (i.e. each bit of Processing that we do).

If we can't identify one of these legal grounds, we shouldn't be doing that Processing.

4.2 Consent

Consent is one of the legal grounds that we can rely on when we Process Personal Data.

What is meant by "Consent" is defined in the GDPR. It needs to be a clear indication of agreement either by a statement or positive action to the Processing by the Data Subject. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient.

If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

Data Subjects must be easily able to withdraw their Consent to Processing at any time. Any withdrawal must be promptly acted upon. Consent may need to be refreshed (i.e. updated) on a regular basis. In addition, the Consent will need to be refreshed if the Group intends to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first gave their Consent.

You will need to evidence Consent captured and keep records of all Consents so that we can demonstrate that we have obtained the right Consent for the right Processing activities. This is part of the accountability principle.

4.3 Transparency (notifying data subjects)

The GDPR requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes or from apprentices/learners, we must provide the Data Subject with all the information required by the GDPR. This is contained in a document called a Privacy Notice.

You will have received our Privacy Notice that sets this information out in relation to your employment/engagement with us. We have to provide a different Privacy Notice to other categories of Data Subject, such as learners.

The Privacy Notice must include the identity of the Data Controller (eg the Group) and our Data Protection Officer ("**DPO**"). It must also set out information about how and why we will use, Process, disclose, protect and retain that Personal Data.

It is important that the Privacy Notice is given at the right time. If the Personal Data is collected directly from the Data Subject, the Privacy Notice must be provided when the Data Subject first provides the Personal Data to the Group.

When Personal Data is collected indirectly (for example, from a third party or publically available source), you must provide the Data Subject with all the information required by the GDPR as soon as possible after collecting/receiving the Personal Data. You must also check that the Personal Data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed Processing of that Personal Data i.e. that the individual knew that their Personal Data was going to be passed to us and for what purposed.

This means that all the third parties that we work with who Process Personal Data collected by the Group should also comply with the GDPR.

A checklist setting out the information that must be included in Privacy Notices is included at the end of this policy (**Appendix A**).

5 Purpose limitation

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

We cannot use Personal Data for new, different or incompatible purposes from those disclosed to the Data Subject when it was first obtained.

This means if we collect Personal Data for one purpose, we shouldn't then use it for another purpose unless we tell the Data Subject what we are going to do and we have a legal ground to undertake that Processing.

6 Data minimisation

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

You may only Process Personal Data when performing your role duties requires it. You cannot Process Personal Data for any reason unrelated to your role duties. If you do use Personal Data for reasons outside your role duties, you may become a Data Controller or Data Processor of that Personal Data and therefore you may have to comply with the terms of the data protection legislation yourself. You could also expose both yourself and the Group to fines and/or a claim for damages from the Data Subject if you have used their Personal Data in a way that was incompatible with the data protection legislation.

You may only collect Personal Data that you require for your role duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes. You shouldn't be collecting any field of Personal Data that is not necessary in the context of the reason you are collecting it.

You must ensure that when Personal Data is no longer needed for specified purposes it is deleted or anonymised, and follow the data retention guidelines we publish from time to time.

7 Accuracy

Personal Data must be accurate and, where necessary, kept up-to-date. It must be corrected or deleted without delay when inaccurate.

You must ensure that the Personal Data we use and hold is accurate, complete, kept up-to-date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

8 Storage limitation

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is Processed.

You must not keep Personal Data in a form where the Data Subject could be identified for longer than needed for the purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

We will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time.

You must ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

9 Security, integrity and confidentiality

9.1 Protecting Personal Data

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data.

You are responsible for helping the Group protect the Personal Data we hold. You must comply with the Group's security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Special Category Personal Data from loss and unauthorised access, use or disclosure.

You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. This includes following the IT specific policies that are published internally from time to time where they are stated to be applicable to you.

If you fail to comply with the Group's security measures (either intentionally or inadvertently), this could lead to disciplinary action against you. This reflects the importance of keeping Personal Data secure.

We may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested. This is to make sure that those third parties adhere to the Group's high standards in relation to the security of Personal Data.

If you are transferring Personal Data to a third party, or if you want to transfer Personal Data to a third party, and you are in any doubt as to whether there is a lawful basis or appropriate contract in place, you should speak to the Data Protection Officer before transferring the Personal Data.

You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

a) Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it. This includes you not accessing certain categories or Personal Data if it is not part of your job profile to do so.

b) Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.

c) Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes. This means that you should not access Personal Data if you are not supposed to.

You must comply with all applicable aspects of our ITS003 IT Services Information Security Policy.

10 Reporting a Personal Data Breach

The GDPR requires Data Controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject.

We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects and/or any applicable regulator where we are legally required to do so. Please refer to our data breach incident management policies and procedures.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the Data Protection Officer at dpo@ltegroup.co.uk.

You should preserve all evidence relating to the potential Personal Data Breach.

If you fail to report a Personal Data Breach in accordance with this policy and associated data breach incident management policies and procedures , this could lead to disciplinary action against you. This is because compliance with these policies and procedures is critical to ensure that any Personal Data Breach is dealt with carefully and promptly to protect the Personal Data of Data Subjects.

11 Transfer limitation

11.1 Data sharing

Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the Personal Data we hold with another employee, agent or representative of our Group if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions (see the section on **International transfers** below for more information on this).

You may only share the Personal Data we hold with third parties, such as our service providers if:

a) they have a need to know the information for the purposes of providing the contracted services;

b) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

d) the transfer complies with any applicable cross border transfer restrictions; and

e) a fully executed written contract that contains GDPR approved third party clauses has been obtained (or another lawful basis has been identified and approved).

A checklist setting out the data protection provisions that must be included in a written contract with our service providers is included at the end of this policy (**Appendix B**).

As above, if you are transferring Personal Data to a third party, or if you want to transfer Personal Data to a third party, and you are concerned that there may not be an appropriate contract in place or are uncertain as to the legal basis upon which the Personal Data is being transferred, you should speak to the Data Protection Officer.

11.2 International transfers

The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

You may only transfer Personal Data outside the EEA if one of the following conditions applies:

a) the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms, a list of countries where a decision has been issued is available at https://ec.europa.eu/info/law/law-topic/data-protection_en;

b) appropriate safeguards are in place, such as: binding corporate rules (BCR); standard contractual clauses approved by the European Commission; an approved code of conduct; or a certification mechanism applies;

c) the Data Subject has provided Consent to the proposed transfer after being informed of any potential risks; or

d) the transfer is necessary for one of the other reasons set out in the GDPR, including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

If you are transferring Personal Data outside of the EEA or if you want to transfer Personal Data outside the EEA, and you are concerned that there may not be an appropriate legal arrangement in place, you should speak to the Data Protection Officer to ensure that an appropriate legal arrangement is in place.

12 Data Subject's rights and requests

Data Subjects have rights when it comes to how we handle their Personal Data.

These include rights to:

a) withdraw Consent to Processing at any time;

b) receive certain information about the Data Controller's Processing activities;

c) request access to their Personal Data that we hold;

d) prevent our use of their Personal Data for direct marketing purposes;

e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

f) restrict Processing in specific circumstances;

g) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

h) request a copy of an agreement under which Personal Data is transferred outside of the EEA;

i) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

j) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

k) make a complaint to the supervisory authority; and

l) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

You must immediately forward any Data Subject request you receive to the Data Protection Officer at dpo@ltegroup.co.uk and comply with the Group's Data Subject response policies and procedures.

A summary of Data Subject's rights under the GDPR is included at the end of this policy (**Appendix C**).

13 Accountability

The Data Controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Data Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

This means that we must have adequate resources and controls in place to ensure and to document GDPR compliance including:

a) appointing a suitably qualified DPO (where necessary) and an executive accountable for data privacy;

b) implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;

c) integrating data protection into internal documents including this Data Protection Policy, Related Policies and Privacy Notices;

d) regularly training you on the GDPR, this Data Protection Policy, Related Policies and data protection matters including, for example, Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. We must maintain a record of training attendance by our Colleagues ; and

e) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

13.1 Record keeping

The GDPR requires us to keep full and accurate records of all our data Processing activities. You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents.

These records should include, at a minimum, the name and contact details of the Data Controller and the DPO, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data

transfers, the Personal Data's retention period and a description of the security measures in place. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

13.2 Training and audit

We are required to ensure that all employees, workers, contractors, agency workers, consultants, directors, members and other individuals who work for and/or are employed by the Group have undergone adequate training to enable them to comply with the data protection legislation. We must also regularly test our systems and processes to assess compliance.

You must undergo all mandatory data privacy related training and ensure your team undergo similar mandatory training in accordance with our mandatory training guidelines.

You must regularly review all the systems and processes under your control to ensure they comply with this Data Protection Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

13.3 Privacy By Design and Data Protection Impact Assessment (DPIA)

We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles.

You must assess what Privacy by Design measures can be implemented on all programs/systems/processes that Process Personal Data by taking into account the following:

a) the state of the art;

b) the cost of implementation;

c) the nature, scope, context and purposes of Processing; and

d) the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

Data Controllers must also conduct DPIAs in respect to high risk Processing (eg if we were to implement a new payroll system)

You should conduct a DPIA when implementing major system or business change programs involving the Processing of Personal Data including:

a) use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

b) large scale Processing of Sensitive Data; and

c) large scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

a) a description of the Processing, its purposes and the Data Controller's legitimate interests if

appropriate;

d) an assessment of the necessity and proportionality of the Processing in relation to its purpose;

e) an assessment of the risk to individuals; and

f) the risk mitigation measures in place and demonstration of compliance.

If you are responsible for the implementation or management of a new project that may require a DPIA, you should speak to the Data Protection Officer in the first instance to ascertain whether a DPIA should be undertaken. If a DPIA is required, you should ensure that this is completed, with the assistance of the Data Protection Officer (if required).

14 Direct marketing

We are subject to certain rules and privacy laws when marketing to learners/potential learners/other "customers".

A Data Subject's prior Consent is generally required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing learners/customers known as "soft opt in" allows us to send marketing texts or emails if we have obtained contact details in the course of a sale to that person, we are marketing similar products or services, and we gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

A Data Subject's objection to direct marketing must be promptly acted upon. If a Data Subject opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

15 Giving references

Nobody should give references in respect of current or past employees of the Group without the prior approval of the Human Resources Department. Any requests for references should be passed to the Human Resources Department in the first instance.

All references (whether oral or written) given in respect of an employee of a Group entity should contain only information that is factual or is an honest opinion or judgement that is capable of being demonstrated as being reasonable by reference to actions or events.

A copy of each reference given should be retained in the staff member's employment record.

Referees should be aware that the content of a reference may, at a future date, be shared with the candidate/employee concerned in accordance with data protection legislation.

16 Definitions of key terms used in this policy

There are lots of terms in this Data Protection Policy which come from the data protection legislation. The following terms have the following meaning:

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Data Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Data Controller of all Personal Data relating to our Colleagues and Personal Data used in our business for our own commercial purposes.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Privacy Impact Assessment (**DPIA**): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

GDPR: the General Data Protection Regulation ((EU) 2016/679)). Personal Data is subject to the legal safeguards specified in the GDPR.

Personal Data: any information relating to an identified or identifiable natural, living, person (Data Subject). An identifiable natural person is someone 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 person. Personal Data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Colleagues: all employees, workers, contractors, agency workers, consultants, directors, members and other individuals who work for and/ or are employed by a Group entity.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Notices: separate notices setting out information that may be provided to Data Subjects when the Group collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the

website privacy policy) or they may be stand-alone, one time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Related Policies: the Group's policies, operating procedures or processes related to this policy and designed to protect Personal Data, referenced in the Reference or Associated Documents section at the beginning of this document (to the extent they are applicable to you and the Group entity you are employed by) and any further policies which are published by the Group from time to time.

17 Changes to this Data Protection Policy

We reserve the right to change this Data Protection Policy at any time so please check back regularly to obtain the latest copy of this Data Protection Policy. We will notify you when we update this policy.

This Data Protection Policy does not override any applicable national data privacy laws and regulations in countries where the Group operates.

Appendix A – Privacy Notice Checklist (GDPR-compliant)

✓	Information to include in Privacy Notice	Notes
	Group entity identity and contact details and details of our representative (if any).	
	Identity and contact details of our data protection officer.	*We are legally required to appoint a data protection officer.*
	The purpose for the processing.	*Avoid generalisations that are open to a variety of interpretations (e.g. "improving user experience", "marketing", "IT security", and "future research").*
	The legal basis for the processing.	*Under the GDPR, it is more difficult to obtain consent and note that public authorities cannot use the legitimate interest basis for processing when performing their tasks carried out in the public interest.*
	Any legitimate interests that we are relying on.	*The recitals to the GDPR identify certain legitimate activities (e.g. processing for preventing fraud, information security and intra-group transfers). However, this must be weighed against individuals' rights and freedoms.*
	The categories of personal data.*	
	Recipients or categories of recipients of the personal data.	*For example, group companies or credit reference agencies.*
	Details of transfers outside the EEA and any safeguards taken.	*The data transfer mechanism used to legalise the transfer must be specified.*
	The period for which data will be retained or the criteria used to determine this period.	
	Details of the data subject's rights.	*This includes the right to be forgotten, restrict processing and to object to processing, the right to data portability and the right to object to direct marketing.*

	The right to withdraw consent at any time (if consent is used as the basis for processing).	*Include details of how the data subject can exercise the right.*
	The right to lodge a complaint with a supervisory authority.	*In the UK, this is the Information Commissioner's Office.*
	The source of the personal data (and whether it was a publicly accessible source).*	
	Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data.**	
	Details of any automated decision making (eg, profiling), the auto-decision logic used, the significance and consequences.	

* not needed where data is obtained directly from data subject

** only needed where data is obtained directly from data subject

Appendix B – Data Processing Contract Checklist

✓	Mandatory provisions for data processing contracts
	Needs to be a binding contract (or legal act) with the processor which sets out the: a) subject matter (eg, the services performed), nature and purpose of the processing (eg, to enable the processor to carry out the services); b) duration of the processing; c) type of personal data; d) categories of data subjects; and e) obligations and rights of controller.
	The processor may only process the personal data in accordance with the controller's documented instructions. There is an exception for processing required by EU or Member State laws.
	The processor must ensure that employees or other people authorised to process the personal data are subject to appropriate obligations of confidentiality.
	The processor must keep the personal data secure (implementing appropriate technical and organisational measures).
	The processor must obtain the controller's consent before using a sub-processor and enter into equivalent data processing obligations with that sub-processor.
	The processor must assist the controller, by technical and organisational measures, with responding to requests from data subjects exercising their rights.
	The processor must assist the controller with complying with the controller's obligations to implement appropriate technical and organisational measures, notify personal data breaches and carrying out data protection impact assessments.
	The processor must delete or return all personal data at the end of the provision of processing services unless EU or Member State Law requires the processor to keep a copy.
	The processor must make available to the controller information to demonstrate compliance with the obligations and allow audits by the controller or its mandated auditor.
	The processor must inform the controller if, in its opinion, the controller's instruction breaches EU or Member State data protection law.

Appendix C – Data Subject rights under the GDPR

Right provided by GDPR	Notes
Right to be informed **See our privacy notice checklist for the details required to be communicated to the data subject.**	If data is obtained **directly from the data subject**, the information should be provided at the time of collection of the data. If data is **not obtained directly** the information should be provided: ✓ within a reasonable period of obtaining the data (within one month); ✓ if the data are used to communicate with the data subject, at the latest, when the first communication takes place; and ✓ if disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
Right of access **Data subjects have the right to obtain:** ✓ **confirmation that their data is being processed;** ✓ **access to their personal data; and** ✓ **other supplementary information – this largely corresponds to the information that should be provided in a privacy notice.**	Information must be provided **without delay** and at the latest within **one month of receipt**. You will be able to extend the period of compliance by a **further two months** where requests are complex or numerous. If so, you must inform the individual within one month and explain why. Where you process a **large quantity** of information about an individual, the GDPR permits you to ask the individual to **specify the information the request relates to**. You must provide a copy of the information **free of charge**. You can charge a **'reasonable fee':** ✓ when a request is manifestly **unfounded or excessive**, particularly if it is repetitive. You could also **refuse to respond** but, without undue delay and within one month, you would have to explain why and inform them of their right to complain and to a judicial remedy; or ✓ to comply with requests for **further copies** of the same information.
Right to rectification **Individuals are entitled to have personal data**	You must respond within **one month** or, if the request is complex, this can be extended by **two months**. **If you are not taking any action**, you must explain why

rectified if it is inaccurate or incomplete.	to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy. If you have disclosed the personal data to **third parties**, you must inform them of the rectification where possible and inform the data subject where appropriate.
Right to erasure **A data subject may request the erasure of personal data where:** **a) the personal data:** ✓ **is no longer necessary in relation to the purpose for which it was originally collected/processed** ✓ **was unlawfully processed** ✓ **has to be erased in order to comply with a legal obligation** ✓ **is processed in relation to the offer of information society services to a child** **b) the individual:** ✓ **withdraws consent** ✓ **objects to the processing and there is no overriding legitimate interest for continuing the processing**	You can **refuse to comply** with a request for erasure where the personal data is processed: ✓ to exercise the right of freedom of expression and information; ✓ to comply with a legal obligation or for the performance of a public interest task or exercise of official authority; ✓ for public health purposes in the public interest; ✓ for archiving purposes in the public interest, scientific research historical research or statistical purposes; or ✓ for the exercise or defence of legal claims. If you have disclosed the personal data to **third parties**, you must inform them about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.
Right to restrict processing **Processing must be suppressed where:** ✓ **the individual contests the accuracy of the personal data;** ✓ **an individual has objected to the processing (where it was necessary for performance of a public interest task or legitimate interests);** ✓ **processing is unlawful and the individual requests restriction instead of erasure;** ✓ **you no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.**	You can continue to store the personal data, but **may only further process it**: ✓ with the data subject's consent; ✓ to establish, exercise, or defend legal claims; ✓ to protect the rights of another individual or legal entity; or ✓ for important public interest reasons. You must inform individuals when you decide to **lift** a restriction on processing. If you have disclosed the personal data to **third parties**, you must inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

Right to data portability **This includes the right to:** ✓ **receive a copy of the personal data, free of charge, from the data controller in a commonly used and machine-readable format and store it for further personal use on a private device;** ✓ **transmit the personal data to another data controller; and** ✓ **have personal data transmitted directly from one data controller to another where technically possible.**	The right to data portability only applies: ✓ to personal data that an **individual has provided** to a controller; ✓ where the processing is based on the individual's **consent or for the performance of a contract**; and ✓ when processing is carried out by **automated means**. You must respond without undue delay and within **one month** or, if the request is complex or there are numerous requests, this can be extended by **two months**. You must **inform the individual of any extension** within one month of the receipt of the request and explain why it is necessary. **If you are not taking any action**, you must explain why to the individual, without undue delay and within one month, informing them of their right to complain to the supervisory authority and to a judicial remedy.
Right to object **Individuals have the right to object to:** ✓ **processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);** ✓ **direct marketing (including profiling); and** ✓ **processing for purposes of scientific/historical research and statistics.**	If processing for the performance of a legal task or legitimate interests, individuals must have an objection on "**grounds relating to his or her particular situation**". You must stop processing the personal data unless: ✓ you can demonstrate **compelling legitimate grounds** for processing, which override the interests, rights and freedoms of the individual; or ✓ the processing is for the establishment, exercise or defence of **legal claims.** If processing for the performance of a legal task or legitimate interests or for direct marketing purposes: ✓ You must inform individuals of their right to object **"at the point of first communication"** and in your **privacy notice**. ✓ This must **be "explicitly brought to the attention** of the data subject and presented clearly and separately from any other information". If processing for direct marketing purposes, there are

	no exemptions or grounds to refuse. If you receive an objection to processing for direct marketing purposes: ✓ you must **stop processing personal data for direct marketing** on receipt; and ✓ you must deal the objection **at any time** and free of charge. If processing for research purposes, individuals must have "**grounds relating to his or her particular situation"** in order to object. You are **not required to comply with an objection** if you are conducting research where the processing of personal data is **necessary for the performance of a public interest task**. If your processing activities fall into any of the specified categories and **are carried out online**, you must offer a way for individuals to object online.
Rights in relation to automated decision making and profiling **Individuals have the right not to be subject to a decision when:** ✓ **it is based on automated processing; and** ✓ **it produces a legal effect or a similarly significant effect on the individual.**	The **right does not apply if** the decision: ✓ is necessary for entering into or performance of a contract between you and the individual; ✓ is authorised by law (eg for the purposes of fraud or tax evasion prevention); ✓ is based on explicit consent (Article 9(2)); or ✓ does not have a legal or similarly significant effect on the individual. You must ensure that individuals are able to: ✓ obtain human intervention; ✓ express their point of view; and obtain an explanation of the decision and challenge it.
Breach Notification Right **When a personal data breach is likely to result in a high risk to a data subject's rights, a data controller must notify the data subject of the security breach without undue delay.**	The breach must be notified without undue delay.

Appendix D – Specific additional policies for certain parts of the Group

Part 1 – Personal Data relating to Children

In addition to the provisions of this policy relating to Group's approach to the Personal Data we Process, Group entities and operating divisions, including in particular The Manchester College and Novus, need to take into account the specific rules applicable to Processing data relating to children.

Data protection legislation requires that children warrant specific protection with regards to Personal Data as they may be less aware of the risks and their rights under the data protection legislation. Compliance with the data protection principles and in particular fairness should be central to all our Processing of children's Personal Data. Checklists to use when children's Personal Data may be Processed are included below, and you should use these to help us comply with the data protection legislation.

Where you wish to collect Personal Data from a child as part of our Information, Advice and Guidance Programme, or as part of our a Novus programme, you need to have a lawful basis for processing a child's Personal Data, in accordance with paragraph 4 of the Group Data Protection Policy. In the case of obtaining Consent, parental consent will be required unless the child is aged 16 years or over.

Children have the same rights as adults over their personal data. These include the rights to access their personal data; request rectification; object to processing and have their personal data erased.

An individual's right to erasure is particularly relevant if they gave their Consent to processing when they were a child.

Checklists

✓	General
	We make sure that our processing is fair and complies with the data protection principles.
	The processor must keep the personal data secure (implementing appropriate technical and organisational measures).
	As a matter of good practice, we use DPIAs to help us assess and mitigate the risks to children.
	If our processing is likely to result in a high risk to the rights and freedom of children then we always do a DPIA.
g	As a matter of good practice, we consult with children as appropriate when designing our processing.

✓	Bases for processing a child's personal data
	When relying on consent, we make sure that the child understands what they are consenting to, and we do not exploit any imbalance in power in the relationship between us.
	When relying on 'necessary for the performance of a contract', we consider the child's competence to understand what they are agreeing to, and to enter into a contract.
	When relying upon 'legitimate interests', we take responsibility for identifying the risks and consequences of the processing, and put age appropriate safeguards in place.

✓	Offering an information Society Service (ISS) directly to a child, on the basis of consent
	If we decide not to offer our ISS (online service) directly to children, then we mitigate the risk of them gaining access, using measures that are proportionate to the risks inherent in the processing.
	When offering ISS to UK children on the basis of consent, we make reasonable efforts (taking into account the available technology and the risks inherent in the processing) to ensure that anyone who provides their own consent is at least 13 years old.
	When offering ISS to UK children on the basis of consent, we obtain parental consent to the processing for children who are under the age of 13, and make reasonable efforts (taking into account the available technology and risks inherent in the processing) to verify that the person providing consent holds parental responsibility for the child.
	When targeting wider European markets we comply with the age limits applicable in each Member State.
	We regularly review available age verification and parental responsibility verification mechanisms to ensure we are using appropriate current technology to reduce risk in the processing of children's personal data.
	We don't seek parental consent when offering online preventive or counselling services to a child.

✓	Marketing
	When considering marketing children we take into account their reduced ability to recognise and critically assess the purposes behind the processing and the potential consequences of providing their personal data.

	We take into account sector specific guidance on marketing, such as that issued by the Advertising Standards Authority, to make sure that children's personal data is not used in a way that might lead to their exploitation.
	We stop processing a child's personal data for the purposes of direct marketing if they ask us to.
	We comply with the direct marketing requirements of the Privacy and Electronic Communications Regulations (PECR).

✓	**Solely automated decision making (including profiling)**
	We don't usually use children's personal data to make solely automated decisions about them if these will have a legal, or similarly significant effect upon them.
	If we do use children's personal data to make such decisions then we make sure that one of the exceptions in Article 22(2) applies and that suitable, child appropriate, measures are in place to safeguard the child's rights, freedoms and legitimate interests.
	In the context of behavioural advertising, when deciding whether a solely automated decision has a similarly significant effect upon a child, we take into account: the choices and behaviours that we are seeking to influence; the way in which these might affect the child; and the child's increased vulnerability to this form of advertising; using wider evidence on these matters to support our assessment.
	We stop any profiling of a child that is related to direct marketing if they ask us to.

✓	Privacy notices
	Our privacy notices are clear, and written in plain, age-appropriate language.
	We use child friendly ways of presenting privacy information, such as: diagrams, cartoons, graphics and videos, dashboards, layered and just-in-time notices, icons and symbols.
	We explain to children why we require the personal data we have asked for, and what we will do with it, in a way which they can understand.
	As a matter of good practice, we explain the risks inherent in the processing, and how we intend to safeguard against them, in a child friendly way, so that children (and their parents) understand the implications of sharing their personal data.

	We tell children what rights they have over their personal data in language they can understand.
	As a matter of good practice, if we are relying upon parental consent then we offer two different versions of our privacy notices; one aimed at the holder of parental responsibility and one aimed at the child.

✓	The child's data protection rights
	We design the processes by which a child can exercise their data protection rights with the child in mind, and make them easy for children to access and understand.
	We allow competent children to exercise their own data protection rights.
	If our original processing was based on consent provided when the individual was a child, then we comply with requests for erasure whenever we can.
	We design our processes so that, as far as possible, it is as easy for a child to get their personal data erased as it was for them to provide it in the first place.

Part 2 – Personal Data relating to Criminal Offences

In addition to the provisions of this policy relating to Group's approach to the Personal Data we Process, Novus and Novus Cambria need to take into account the specific rules applicable to Processing criminal offence data.

The GDPR rules for sensitive (special category) data do not apply to information about criminal allegations, proceedings or convictions. Instead, there are separate safeguards for personal data relating to criminal convictions and offences, or related security measures.

To process personal data about criminal convictions or offences, you must have both a lawful basis in accordance with paragraph 4 of this policy and either legal authority or official authority for the processing in accordance with the data protection legislation.

We cannot keep a comprehensive register of criminal convictions unless we are required to do so in an official capacity.

You must determine the condition for lawful processing of offence data and identify the legal authority for the processing before you begin the processing, and you should document this.

Further information about Processing criminal offence data will be published when the new UK Data Protection Act is passed.

Part 3 – International transfers of Personal Data in the context of online learning

In addition to the provisions of this policy relating to Group's approach to the Personal Data we Process, Group entities and operating divisions, including in particular MOL, need to take into account the specific rules applicable to Processing data relating to individuals who are based worldwide.

In this Part 3:

"**International Organisation**" have the same meaning as in the data protection legislation; and

"**Third Country**" means any country other than the UK, a European Union Member State or a member of the European Economic Area at the time of transfer of Personal Data.

Individuals around the world are able to access and enrol online to the MOL courses by submitting their Personal Data. We still have to adhere to the data protection legislation despite the Data Subject being based outside of the European Union.

Where you wish to transfer Personal Data to an individual based outside of the EEA pursuant to enquiries raised, you should identify the legal basis (in accordance with paragraph 4 of this Group Data Protection Policy) on which that Personal Data is being transferred under the data protection legislation and determine which of the conditions set out in paragraph 11.2 applies before such transfer takes place.

As stated in paragraph 11.2, the GDPR requires adequate and appropriate safeguards put in place before an international transfer of personal data takes place. However, there are derogations which apply to such transfers, in the following circumstances (in the absence of adequacy determinations or appropriate safeguards):

a) The individual has explicitly consented after being informed of the risks of the transfers due to the absence of an adequacy decision and appropriate safeguards.
b) It is necessary for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request.
c) It is necessary for the performance of a contract made in the interests of the individual between the controller and another person.
d) It is necessary to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving consent.
e) It is necessary for important reasons of public interest or to establish, exercise or defend legal claims.
f) The transfer is made from a public register which is intended to provide information to the public and specific conditions are fulfilled.
g) The transfer is in the Controller's legitimate interests. This can only apply if no other derogations are applicable; in respect of occasional transfers concerning only a limited number of data subjects which are necessary for the legitimate interests of the data controller. The data controller is additionally required to provide appropriate safeguards for the personal data and to

inform both the supervisory authority and the data subjects of the transfer. The assessment and the safeguard applied must be documented.

These derogations may be applicable to the international transfers undertaken by MOL.

In the event of any international transfer of Personal Data, it will be necessary to enter into a legally binding agreement between the parties involved in the transfer before the transfer of data takes place.

Please contact the Data Protection Officer if you have any queries about international transfers in the context of MOL's distance learning activities.