Data Protection Policy

Document Control	
Document Type:	Policy
Department:	Data Protection
Relevancy:	Group-wide
Owner:	Assistant Data Protection Officer
Approver:	LTE Group Board
Published Date:	
Version:	2
Security Classification:	External
Last Review Date:	May 2022
Next Review Date:	June 2024

Version history

Version	Date	Revisions
1.0	July 2019	
2.0	May 2022	Triennial policy review

Contents

Introduction

LTE Group (the "**Group**") includes MOL, Novus, Novus Cambria, The Manchester College, Total People and UCEN Manchester. The Group is committed to protecting the rights and privacy of individuals in accordance with the General Data Protection Regulation (GDPR) and Data Protection Act 2018. The purpose of this Policy is to help you understand the Group's obligations under Data Protection Legislation to enable LTE Group to comply with the law.

This Policy sets out the responsibilities of the Group, including colleagues and students. These responsibilities are to be adhered to by all colleagues while employed by and Processing data on behalf of LTE Group, however the principles are also applicable post-employment (as detailed in section 170 of the Data Protection Act 2018 in respect of a person misusing data without the Consent of the Data Controller).

The Information Commissioner's Office ("**ICO**") is the supervisory authority regulating data protection in the United Kingdom. Both LTE Group and Total People are registered with the ICO as organisations Processing Personal Data. Breaches of Data Protection Legislation 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 colleagues fail to comply with the requirements of this Policy and the Related Policies they may be subject to disciplinary action.

Some parts of Data Protection Legislation can sound quite technical and legal, particularly because of the various legal definitions and phrases that are used. We have therefore included a table of Definitions" at the end of this Policy (Annex 2).

Any questions or concerns about the interpretation or operation of this Policy should be referred to the Data Protection Officer:

Data Protection Officer
LTE Group
Whitworth House
Ashton Old Road
Manchester
M11 2WH

dpo@ltegroup.co.uk

1. Scope

The GDPR applies to the **Processing** of **Personal Data** by automated means or where Personal Data form, or are intended to form, part of a structured filing system. As LTE Group are classed as a public body subject to the Freedom of Information Act (FOIA) 2000, the GDPR also applies to the manual unstructured Processing of Personal Data held by LTE Group.

1.1. Roles and responsibilities

LTE Group Board	The LTE Group Board are responsible for appointing a Data Protection Officer and ensuring that the Data Protection Officer receives the necessary support to undertake the role and maintain their expert knowledge.
General Counsel and Company Secretary	As the registered Data Protection Officer, the General Counsel and Company Secretary is responsible for ensuring overall compliance with the Group's data protection strategy.
Assistant Data Protection Officer	The Assistant Data Protection Officers are responsible for the day-to-day implementation of the data protection strategy.
Colleagues	All colleagues have a duty to ensure they take responsibility for adhering to this Policy and that they work in accordance with Data Protection Legislation when engaging in any data Processing.
Data Subjects	As Data Subjects, all colleagues, students and other relevant parties are responsible for ensuring that any Personal Data they supply about themselves to the Group is accurate and up to date.

1.2. 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, 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.

LTE Group uses Personal Data in relation to various types of Data Subject, including Employees, students, applicants, business contacts, third party stakeholders, suppliers, and contractors.

1.3. Special Category Personal Data

There are special categories of Personal Data which attract higher levels of protection under GDPR:

- Personal Data revealing racial or ethnic origin;

- Personal Data revealing political opinions;
- Personal Data revealing religious or philosophical beliefs;
- Personal Data revealing trade union membership;
- Genetic data;
- Biometric data (where used for identification purposes);
- Data concerning health;
- Data concerning a person's sex life;
- Data concerning a person's sexual orientation.

In order to Process Special Category Data, we must identify both a Lawful Basis under Article 6 of the GDPR and a separate condition for Processing under Article 9. The DPO will document these Lawful Bases on the relevant Information Asset Registers and Privacy Notices.

1.4. Criminal Offence Data

Personal Data relating to criminal offences and convictions also attracts separate and specific safeguards. The Processing of Criminal Offence Data or related security measures shall be carried out only under the control of official authority or when Processing is authorised by law, providing for appropriate safeguards for the rights and freedoms of Data Subjects (Article 10 GDPR). The Data Protection Act 2018 deals with this type of data in a similar way to Special Category Data and sets out specific conditions providing lawful authority for Processing it.

1.5. What does "Processing" Personal Data mean?

Data Protection Legislation only applies to the "Processing" of Personal Data.

Processing has a broad definition and includes almost any action performed on Personal Data, including obtaining, recording, organising, structuring, holding, using, disclosing, and destroying Personal Data.

1.6. Who is the "Data Controller" and "Data Processor"?

A "**Data Controller**" determines the purpose and means of Personal Data Processing. LTE Group will typically be a Data Controller for all student and colleague Personal Data. Under Data Protection Legislation, the Group and each Business Unit are classed as Data Controllers in their own right.

A "**Data Processor**" is any person who Processes data on behalf of the Data Controller. As a Data Controller, we remain responsible for Personal Data that we share with any Data Processor. We are required to put in place a written contract (Data Sharing Agreement) with any Data Processor 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 share data belonging to LTE Group with a third party must speak to the Data Protection Officer to ensure that an appropriate contract or Data Sharing Agreement is put in place.

Colleagues carrying out their role while working for the Group are not classed as Data Processors. However, if colleagues act outside of their contract or role, they may become

a Data Controller or Data Processor, and the legal obligations that fall to the Group as Data Controller could equally apply to the colleague.

2. The Data Protection Principles

The GDPR sets out seven key Principles in relation to Processing Personal Data:

a) Lawfulness, Fairness and Transparency
b) Purpose Limitation
c) Data Minimisation
d) Accuracy
e) Storage Limitation
f) Security, Integrity and Confidentiality
g) Accountability

We are responsible for, and must be able to demonstrate, compliance with the above Principles

Lawfulness, fairness and transparency Personal Data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.	**Lawfulness and fairness** The GDPR only allows Processing for specific purposes. These are known as the Lawful Basis of Processing. As a Data Controller, we need to comply with at least one of these grounds to ensure the Processing is lawful and compliant with Data Protection Legislation. The Lawful Bases are: a) the Data Subject has given **Consent** b) the Processing is necessary for the performance of a **contract** with the Data Subject c) necessary to meet our **legal obligations** d) in order to protect the Data Subject's **vital interests** e) to provide performing a task in the **public interest** f) to pursue **legitimate interests** where the Processing does not prejudice the interests or fundamental rights of Data Subjects. Information about our Lawful Bases are outlined in our Privacy Notice. They are also documented in our Information Asset Registers and/or Data Sharing & Contracts Register, which is owned by the Data Protection department. It is important that colleagues make the DPO, or their local Data Protection Champion, aware of any changes to the way Personal Data is being Processed. **Transparency** Whenever we collect Personal Data directly from Data Subjects, we must provide the Data Subject with certain information. This information is contained in a document called a Privacy Notice. The Privacy Notice must include the identity of the Data

	Controller and our Data Protection Officer. It must also set out information about how and why we will use, Process, disclose, protect, and retain Personal Data. LTE Group's Privacy Notices are available on our websites and on the colleague intranet (HUB). It is important that the Privacy Notice is provided in a timely manner. If the Personal Data is collected directly from the Data Subject, the Privacy Notice must be provided at the point when the Data Subject initially provides the Personal Data. When Personal Data is collected indirectly (for example, from a third party or publicly available source), we must provide the Data Subject with the Privacy Notice as soon as possible after collecting/receiving the Personal Data. We 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, e.g. that the individual knew that their Personal Data was going to shared with us and for what purpose. Colleagues are advised to liaise with the DPO to undertake such checks.
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 will not then use it for another purpose unless we notify the Data Subject what we are going to do and we have a Lawful Basis to undertake the new Processing.
Data minimisation Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.	Colleagues may only Process Personal Data when performing their job responsibilities requires it. Personal Data cannot be Processed for any reason unrelated to a colleague's job responsibilities. Personal Data should only be collected where genuinely required: colleagues should not collect excessive categories of data. Personal Data must be adequate and relevant for the intended purposes. When Personal Data is no longer needed for its specified purpose, it must be deleted or anonymised in line with the published data retention guidelines.
Accuracy Personal Data must be accurate and, where necessary, kept up-to-date. It must be	**Colleagues must:** - ensure that the Personal Data is accurate, complete, kept up-to-date and relevant to the purpose for which it was collected - check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards - take all reasonable steps to destroy or amend inaccurate or

corrected or deleted without delay when inaccurate.	out-of-date Personal Data **Data Subjects must:** ensure that the data we hold for them is accurate and up to date and notify us of any changes to their data in a timely manner.
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.	Personal Data must not be kept in a form where the Data Subject could be identified for longer than needed for the purpose for which we originally collected it, including for the purpose of satisfying any legal, accounting or reporting requirements. LTE Group 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 amount of time. LTE Group will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in the applicable Privacy Notice.
Security, integrity and confidentiality Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.	The Group 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 and identified risks. We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data. All colleagues are responsible for helping the Group protect the Personal Data we hold. Colleagues 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. These are also referenced wherever applicable in other Relevant Polices and documents. Colleagues must exercise particular care in protecting Special Category Personal Data and Criminal Offence Data from loss and unauthorised access, use or disclosure. All colleagues and students must follow all relevant procedures and requirements around technologies to maintain the security of Personal Data. This includes following the IT-specific policies that are published and where applicable. For colleagues, failure to comply with the Group's security measures (either intentionally or inadvertently), could lead to disciplinary measures. LTE Group will 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 ensure that those third parties adhere to

	the Group's high standards in relation to the security of Personal Data. Colleagues transferring, or intending to transfer, Personal Data to a third party should ensure that the appropriate security measures are in place and, if in doubt, liaise with the Data Protection Officer before any transfer takes place. All colleagues 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 colleagues not accessing certain categories or Personal Data if it is not part of their 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 colleagues should not access Personal Data if they are not supposed to. Colleagues must comply with all applicable aspects of our ITS003 IT Services Information Security Policy and Acceptable Use Policy.
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.	Accountability 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) providing regular training on GDPR, this Policy, Related Policies and data protection matters including, for example, Data Subject's rights, Consent, legal bases, DPIA and Personal Data Breaches; 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.

Record keeping

The GDPR requires us to keep full and accurate records of all our data Processing activities. Colleagues must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consent and procedures for obtaining Consent. LTE Group maintains Information Asset Register for each Business Unit, which are managed by the DPO and Data Protection Champions. If anything should change in the way colleagues Process data, colleagues should notify the DPO or their local Data Protection Champion immediately.

Records of Processing should include, at a minimum, 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.

Training and audit

Data Controllers are required to ensure that all Employees, workers, contractors, agency workers, consultants, directors, members, and other individuals Processing Personal Data 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.

All Group colleagues must undertake all mandatory data privacy related training assigned to them.

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

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.

We must assess what Privacy by Design measures can be

	implemented for 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. The DPO will work with relevant colleagues to 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. Where colleagues are responsible for the implementation or management of a new project that may require a DPIA, they should always speak with the DPO in the first instance to ascertain whether a DPIA should be undertaken. Colleagues should refer to the DPIA guidance for further information on when and how to conduct a DPIA.

3. Individual Rights and requests

Under GDPR, Data Subjects have a range of Individual Rights in relation to how organisations Process their Personal Data.

These include:

1. **The right to be informed** about the collection and use of their Personal Data (for example, through the Privacy Notice).
2. **The right of access** to copies of their Personal Data; this is also known as a Subject Access Request.

3. **The right to rectification** where Data Subjects believe their Personal Data is inaccurate, this includes asking us to complete information where they believe it is incomplete.
4. **The right to erasure** (in certain circumstances), for example, if it is no longer necessary for the Group to hold Personal Data in relation to the original purposes for Processing.
5. **The right to restrict Processing** (in certain circumstances).
6. **The right to data portability** (in certain circumstances). Data Subjects can ask that the Group transfers their Personal Data to another organisation, or to them.
7. **The right to object** to our Processing of their Personal Data (in certain circumstances).
8. **Rights in relation to Automated Decision-Making and profiling**, where we undertake any decision making without human intervention, or profiling of, the Data Subject.

3.1. Processing Individual Rights requests

All Individual Rights requests must be processed by the DPO.

A request can be made verbally or in writing and should be addressed to the Data Protection Officer but can be made to any Group colleague/department. Requests may not expressly refer to GDPR or Individual Rights requests. They may be submitted, for example, as part of a conversation, or as part of a complaint and do not need to refer to Data Protection Legislation. If any individual asks to see "all information that we hold about them", this will be a Subject Access Request.

Under Data Protection Legislation, we must respond to all Individual Rights requests within 30 days of the request being submitted. Therefore, if a colleague or department receives a request that falls under the above rights, they must immediately forward the request to the DPO: dpo@ltegroup.co.uk, to ensure that the response is not delayed. If colleagues are unsure whether the request is an Individual Rights request, they must still forward it to the Data Protection Officer, for assessment.

The Data Protection department will process and respond to all Individual Rights requests. The DPO may need to identify the person making the request and verify their right to receive such information.

In certain circumstances, Individual Rights requests can be refused. In such cases this will be determined and communicated to the requestor by the DPO.

4. Data Security Incidents, Data Breaches, Suspected Breaches and Near Misses

If any colleague or person associated with the Group (e.g., student, stakeholder) becomes aware or suspects that a Personal Data Breach has occurred, they must immediately notify the DPO at dpo@ltegroup.co.uk and preserve all evidence relating to the potential Breach.

This applies irrespective of how minor the incident is believed to be. The DPO will log and assess the incident and initiate any necessary control measures to reduce or mitigate any harm or potential harm arising. It is essential that any such incidents are reported without delay, as the GDPR imposes a statutory timeframe in which to report the incident to the ICO (where applicable).

Reports of Data Security Incidents will always be received and handled in confidence.

Please refer to the data breach procedure should you suspect a Personal Data Breach has occurred. It is important that this process is followed and without undue delay to ensure compliance with Data Protection Legislation. The DPO have measures in place 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.

For colleagues, failure to report a Personal Data Breach in accordance with this Policy and associated policies and procedures, could lead to disciplinary measures.

5. Transfer limitation

5.1. Data sharing

We will not share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place and the sharing is necessary for the lawful purpose of the Processing.

The Student Personal Data Disclosure GDPR Toolkit outlines the processes that colleagues are expected to follow in relation to sharing student Personal Data with third parties. A GDPR Toolkit for disclosure of colleague data is in development.

Colleagues must only share Personal Data with other Employees, agents or representatives of the Group if the Recipient has a role-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions (see: International transfers below for more information).

Personal Data may only be shared if:

a) the Recipient has a need to know the information for the purposes of providing contracted services;
b) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject;
c) the Recipient has agreed to comply with the required data security standards, policies and procedures and has 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).

It may also be appropriate to put a Data Sharing Agreement in place, setting out the nature of the sharing and data protection provisions service providers. More information on data sharing is available on the Data Sharing KnowHow tile on HUB.

As above, where colleagues 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, advise should be sought from the DPO.

5.2. International transfers

The UK GDPR restricts data transfers to countries outside of the UK and EU, in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. International transfers occur where Personal Data originating in one country crosses borders when it is transmitted, sent, viewed or accessed in or to a different country.

Any intended international transfers of Personal Data must be approved by the DPO. LTE Group will only transfer Personal Data outside of the UK/EU 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; international data transfer agreements (IDTA); 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.

6. Direct Marketing

We are subject to certain rules and privacy laws when Direct Marketing to our applicants, students, alumni, and any other potential service user. If we send electronic marketing messages (by phone, fax, email or text), use website cookies, or provide electronic communication services to the public, we must do so in accordance with the Privacy and Electronic Communications (EC Directive) Regulations (PECR) 2003. It is important that colleagues leading on activities defined as Direct Marketing or electronic communications do so in conjunction with the Data Protection department to ensure the activity meets compliance requirements.

A Data Subject's prior Consent is generally required for electronic Direct Marketing (for example, by email, text or automated calls).

There is a limited exception for existing service users known as the "soft opt-in" rule. Soft opt-in allows us to undertake Direct Marketing if we have obtained contact details in the course of an enquiry to our Group’s services where 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 each subsequent correspondence.

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.

7. Changes to this Policy

We reserve the right to make changes to this Data Protection Policy at any time.

This Policy does not override any Data Protection Legislations or regulations in countries where the Group operates. This Policy shall be updated in line with any additions or amendments to relevant laws and regulations in a timely fashion.

This Policy was approved on 20 June 2022 by the LTE Group Board and will be reviewed in June 2024.

8. Further information

Any queries relating to this Policy and its implementation should be raised with the Data Protection department: dpo@ltegroup.co.uk

If any Data Subject is not satisfied with the way LTE Group has Processed their Personal Data, they have the right to lodge a complaint with the Information Commissioner's Office. The Information Commissioner can be contacted at:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

or

https://ico.org.uk/make-a-complaint/

Related Policies and documents

- Acceptable Use Policy - Colleagues
- Data Protection Dos and Don'ts
- Data Protection Impact Assessment Template
- Data Protection Impact Assessment Guidance
- Data Protection Incident Procedure
- Data Retention Schedule
- GDPR Toolkit – Direct Marketing
- GDPR Toolkit – Photography & Videography
- GDPR Toolkit – Student Personal Data Disclosure
- ITS003 LTE Group IT Services Information Security Policy
- ITS007 LTE Group IT Services Encryption Policy
- ITS011 LTE Group IT Services Access Control Policy
- ITS027 LTE Group IT Services Clear Desk Policy
- ITS028 LTE Group Information Security Policy Statement
- ITS039 LTE Group IT Services Disposal and Re-Use of Media Policy
- ITS042 LTE Group IT Services Network Security Policy
- ITS068 LTE Group IT Services Password Policy
- ITS099 LTE Group IT Services Information Exchange Policy
- ITS111 LTE Group IT Services System Configuration Policy
- ITS169 LTE Group Bring Your Own Device Policy
- NOV008 – Novus Information Security Policy Statement
- NOV016 – Novus Data Retention, Archiving & Disposal Policy
- NOV023 – Novus Password Policy
- NOV024 – Novus Information Classification & Handling Policy
- NOV034 – Novus Bring Your Own Device (BYOD) Policy
- NOV035 – Novus Information Exchange Policy
- NOV045 – Novus Retention and Archiving Guidance
- Privacy Notices – Colleagues
- Privacy Notices - Students
- Records Management Policy

Definitions

Automated Decision-Making	When a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.
Business Unit	A distinct Business Unit with LTE Group, such as: Total People, MOL, Novus, UCEN, The Manchester College, Group Ops.
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.
Criminal Offence Data	Any data relating to the outcome of a criminal proceeding in which an individual is found guilty of the crime with which they are charged. See: Criminal Offence Data.
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.
Data Processor	A natural or legal person, public authority, agency, or other body which Processes Personal Data on behalf of the controller.
Data Protection Impact Assessment (DPIA)	Tools and assessments used to identify and reduce risks of a data Processing activity. A 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.
Data Protection Legislation	Means (a) any law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding restriction (as amended, consolidated or re-enacted from time to time) which relates to the protection of individuals with regards to the Processing of Personal Data to which a party is subject, including the Data Protection Act 2018 ("DPA"), the General Data Protection Regulation (GDPR), the Privacy and Electronic Communications Regulations (PECR), and all legislation enacted in the UK in respect of the protection of Personal Data; and (b) any code of practice or guidance published by the ICO (or equivalent regulatory body) from time to time.
Data Protection Officer (DPO)	The person whose responsibility is to ensure the Data Controller is appropriately protecting the Personal Data of individuals in line with Data Protection Legislation.
Data Sharing & Contracts Register	A register containing an overview of organisations with who we share Personal Data with. The Register contains the categories of Personal Data, Lawful Basis, Contract Lead, etc.
Data Sharing Agreement	Sets out the purpose of the data sharing, cover what happens to the data at each stage, set standards and help all the parties involved in sharing to be clear about their roles and responsibilities.
Data Subject	A living, identified, or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country.

Direct Marketing	The communication (by whatever means) of any advertising or marketing material which is directed to particular individuals.
Employee	All employees, workers, contractors, agency workers, consultants, directors, members, and other individuals who work for and/or are employed by the Group.
Explicit Consent	Consent which requires a very clear and specific statement.
Individual Rights	Certain rights provided to individuals under Data Protection Legislation.
Information Asset Register	A database which holds details of all the information assets within an organisation. This can include listing physical assets such as paper files, computer systems and even people as well as, importantly; the data itself, and how it is stored, Processed and shared.
Information Commissioner (ICO)	The regulator for data protection in the UK: the Information Commissioner's Office, or any successor or replacement supervisory authority from time to time.
Lawful Basis or Lawful Bases	Data Protection Legislation requires any organisation Processing Personal Data to have a valid legal basis for that Personal Data Processing activity, set out under Article 6 GDPR.
Personal Data	Any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. 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.
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.
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.
Recipient	The receiver of Personal Data, where the Personal Data has been sent to somebody by a Data Controller.
Relevant or Related Policies	Policies or procedures which are relevant to this Data Protection Policy, a table of which is available at the end of this Policy.
Special Category Personal Data	Information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data. Special Category Data is Personal Data that needs more protection because it is sensitive. See: Special Category Data.
Subject Access Request	Individuals' right to access and receive a copy of their Personal Data, and other supplementary information.
Suppressed	Rather than deleting an individual's details entirely, suppression involves retaining just enough information to ensure that their preferences are respected in the future. Suppression allows organisations to ensure that they do not send Direct Marketing to people who have previously asked them not to, as there is a record against which to screen any new marketing lists. If individuals' details are deleted entirely, there is no way of ensuring that they are not put back on the database.