DATA PROTECTION POLICY

CONTENTS:

N

1. Purpose

1.1 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.

1.2 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).

1.3 This document has been written with regard to the UK GDPR and the Data Protection Act 2018 ("DPA 18"), collectively "Data Protection Regulations".

2. Scope

2.1 This document applies to all business units, and to all colleagues of The Group. It is the responsibility of all colleagues to ensure that any personal data they handle is done so in accordance with this policy.

2.2 This document applies to all personal data processed by The Group, whether in physical or digital form, and regardless of the type of media on which the personal data is stored.

2.3 This document applies to personal data processed by The Group where it is acting as either a data controller or data processor.

2.4 Under the data protection regulations, The Group is required to demonstrate compliance with the principles set out in Article 5 of the UK GDPR. This document is intended to aid in fulfilling this obligation.

3. Roles and Responsibilities

3.1 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.

3.2 As the registered Data Protection Officer, the General Council and Company Secretary is responsible for ensuring overall compliance with The Group's data protection strategy.

3.3 The Assistant Data Protection Officers ("ADPOs") are responsible for the day-to-day implementation of the data protection strategy.

3.4 All colleagues have a duty to ensure that they read, understand, and adhere to this policy, and that they work in accordance with data protection regulations when handling personal data.

3.5 As data subjects, all colleagues, students, and other relevant parties are responsible for ensuring that any personal data that they supply about themselves to The Group is accurate and up to date.

4. Data Protection by Design and Default

4.1 The UK GDPR requires that The Group put in place appropriate technical and organisational measures to implement the data protection principles effectively and safeguard individual rights.

4.2 This principle is Data Protection by Design and Default and is now a legal requirement under data protection

N

regulations.

4.3 This requires that data protection must be integrated into The Group's processing activities and business practices, from the design stage through the full lifecycle.

4.4 The Group maintains a Data Protection by Design and Default Policy, which sets out our obligations with regard to this principle.

4.5 All colleagues are responsible for complying with the Data Protection by Design and Default Policy, and failure to comply may lead to disciplinary measures.

5. Principles

5.1 The UK GDPR sets out six key principles which govern how personal data must be processed, as well as a seventh principle which applies to data controllers such as The Group.

5.2 These principles are as follows:

5.3 **Lawfulness, fairness, and transparency**

5.3.1 For The Group's processing of personal data to be considered lawful and fair, we are required to identify a lawful basis from Article 6 of the UK GDPR for each processing activity we undertake.

5.3.2 If the processing activity involves the use of special category personal data, The Group must identify an additional lawful basis from Article 9 of the UK GDPR.

5.3.3 The Lawful bases for processing are detailed in Appendix B of this document.

5.3.4 For the processing of personal data to be considered transparent, data subjects must be informed about how The Group processes their data.

5.3.5 Such information is provided in the form of Privacy Notices, which set out how and why we process personal data, any organisations to whom we disclose personal data, and details as to the rights that data subjects have in relation to their data.

5.3.6 Each of the business units in The Group has its own privacy notices, which are available on the HUB, as well as being published on the websites of the business units.

5.3.7 Privacy notices must be provided to data subjects in a timely manner, usually at the point at which The Group collects their personal data.

5.3.8 Where personal data is collected indirectly (e.g. from a third party or publicly available source), The Group must provide the data subject with the privacy notice as soon as possible after collecting or receiving the data.

5.3.9 The Group has a duty to ensure that any personal data provided by a third party was collected in accordance with data protection regulations, and on a basis which is compatible with our proposed processing of the data.

5.4 **Purpose Limitation**

5.4.1 The Group must be clear and transparent regarding the purposes for which it is collecting personal data.

5.4.2 Unless under specific circumstances, the Group must not process personal data for a different purpose

N

than that for which the data was originally collected.

5.4.3 A change in purpose of processing is only permitted if:

5.4.3.1 The new purpose is compatible with the original purpose;

5.4.3.2 The Group gains the consent of the data subject; or

5.4.3.3 The processing is required for a clear obligation or function set out in law.

5.4.4 If the purpose of processing does change, The Group must notify the data subjects of this change as soon as possible.

5.4.5 Determination of whether the purpose of processing for a given set of personal data can change is ultimately the responsibility of the risk owner for the project or activity, but a change of purpose must not take place without consultation with the DPO.

5.5 **Data Minimisation**

5.5.1 Personal data may only be processed by The Group where it is:

5.5.1.1 Adequate – sufficient to fulfil our stated purpose;

5.5.1.2 Relevant – is required for our stated purpose; and

5.5.1.3 Limited to what is necessary – We must not hold more personal data than what is require for our stated purpose.

5.5.2 This means that The Group must only collect personal data where it is required for a specific purpose.

5.5.3 It is not permitted for The Group to collect personal data for unspecified purposes, or for an undefined future need.

5.6 **Accuracy**

5.6.1 The Group must take all reasonable steps to ensure that the personal data we process is not incorrect or misleading as to any matter of fact.

5.6.2 In general, The Group is required to ensure that personal data held is kept up to date.

5.6.3 If we discover that personal data we hold is inaccurate, we must take reasonable steps to ensure that it is corrected or removed as soon as possible.

5.7 **Storage Limitation**

5.7.1 Personal data must only be stored for as long as it is needed for the purposes of processing.

5.7.2 Retention of personal data is permitted in order to fulfil any legal, accounting, or reporting requirements to which The Group is subject.

N

5.7.3 The Group maintains a Records Management Policy which sets out the manner in which data should be handled.

5.7.4 The Group Data Retention Schedule specifies for how long each type of personal data The Group processes should be held, as well as the justification for each retention period.

5.8 **Integrity and Confidentiality (Security)**

5.8.1 Personal data processed by The Group must meet the following criteria:

5.8.1.1 Confidentiality – only colleagues or third parties who have a need to know, and are authorised to use, the personal data are permitted to access it. This includes colleagues not accessing certain categories of personal data if it is not part of their job role to do so.

5.8.1.2 Integrity – Personal data must be accurate and suitable for the purpose for which it is processed.

5.8.1.3 Availability – Authorised users must be able to access personal data when it is needed for authorised purposes. A loss of access when it is needed is considered to be a breach of this principle.

5.8.2 The Group must process personal data in a manner that ensures appropriate security from being revealed, disseminated, accessed, or manipulated.

5.8.3 The Group must develop, implement, and maintain safeguards to ensure that personal data is appropriately secured. Such safeguards must be evaluated and tested on a regular basis.

5.8.4 All colleagues of the Group must ensure that the comply with The Group's security measures against unlawful or unauthorised processing of personal data.

5.8.5 All colleagues must follow all relevant policies, procedures and requirements around technologies to maintain the security of personal data

5.8.6 Failure to comply with The Group's security measures, either intentionally or inadvertently, could lead to disciplinary measures for colleagues.

5.8.7 LTE Group must only use processors who comply with data protection regulations, and whose measures around the security of personal data are judged to be adequate.

5.8.8 Any transfer of personal data to a third party must be protected by appropriate security measures. Where the security of a proposed data transfer is in doubt, colleagues must consult the DPO before the transfer takes place.

5.8.9 Colleagues are required to comply with all aspects of the IT Services Information Security Policy, and the Acceptable Use Policy.

5.9 **Accountability**

5.9.1 The Accountability principle requires that The Group take responsibility for our processing of personal data, and how we comply with the other principles.

5.9.2 The Group is required to have appropriate measures and records in place in order to demonstrate our compliance. These measures include:

N

5.9.2.1 Adopting and implementing data protection policies and procedures;

5.9.2.2 Taking a 'data protection by design and default' approach;

5.9.2.3 Having in place written contracts where third parties process personal data on The Group's behalf;

5.9.2.4 Maintaining documentation of our processing activities;

5.9.2.5 Implementing appropriate security measures to protect the personal data we process;

5.9.2.6 Recording and, where necessary, reporting personal data breaches;

5.9.2.7 Carrying out DPIAs for uses of personal data which are likely to result in a high risk to the rights and freedoms of data subjects;

5.9.2.8 Appointing a Data Protection Officer; and

5.9.2.9 Adhering to relevant codes of conduct and signing up to certification schemes.

5.9.3 The Group's accountability obligations are ongoing and require regular review and update of the measures that are put in place to meet them.

5.9.4 The Group is required to provide data protection to all colleagues who handle personal data as part of their role, in order to ensure that they are able to comply with data protection regulations.

5.9.5 Data protection training is mandatory for all such colleagues, and failure to complete said training could lead to disciplinary measures.

5.9.6 The Group maintains an Information Asset Register for each business unit, which must contain the following:

5.9.6.1 A clear description of each type of personal data processed;

5.9.6.2 The categories of data subjects;

5.9.6.3 A clear description and purpose for each processing activity;

5.9.6.4 Any third parties to whom personal data is transferred;

5.9.6.5 The storage locations of each type of personal data;

5.9.6.6 The retention period for each type of personal data; and

5.9.6.7 A description of any security measures in place for the personal data.

6. The Group as a Data Processor

6.1 Where The Group is acting as a data processor, we must only process personal data in accordance with the instruction of the data controller.

6.2 Such instructions will be documented in the contract between The Group and the data controller.

6.3 The Group must only use sub-processors set out in the contract, or subsequently approved by the data controller.

6.4 The Group is responsible for assisting the data controller in complying with its obligations under data

N

protection regulations, the terms of which will be set out in the contract.

6.5 The Group will provide all information reasonably required by the controller to demonstrate The Group's compliance with data protection regulations.

6.6 The Group will participate in audits by the data controller as reasonably required for compliance with the Accountability Principle.

6.7 Upon expiry or termination of the contract, The Group will be required to return or destroy relevant personal data, as set out in the contract.

7. Data Protection Impact Assessments

7.1 As part of The Group's obligations arising from the accountability principle, there are certain circumstances under which a Data Protection Impact Assessment ("DPIA") must be undertaken.

7.2 A DPIA is a process designed to help a controller or processor systematically analyse, identify, and minimise the data protection risks of a project or plan.

7.3 In addition to potentially being required for new projects, DPIAs may need to be completed for existing projects where they meet the requirements and a DPIA is not already in place.

7.4 DPIAs must be reviewed on a regular basis and, regardless, when any change to a project or plan includes a change in the way personal data is processed.

7.5 The Group maintains a Data Protection Impact Assessment Policy, which sets out our obligations, guidance on when DPIAs are required, and the expectations for colleagues with regard to DPIAs.

7.6 Colleagues are responsible for complying with the Data Protection Impact Assessment Policy, and failure to comply may lead to disciplinary measures.

8. Data Sharing

8.1 The Group must not share personal data with third parties unless certain safeguards and contractual arrangements have been put in place.

8.2 The Group must not share personal data with third parties unless the sharing is strictly necessary for the purposes of processing.

8.3 Personal data may only be shared with third parties if:

8.3.1 The recipient is required to process the personal data to achieve the purposes or processing;

8.3.2 Sharing the personal data complies with the privacy notice provided to the data subject;

8.3.3 The recipient has agreed to comply with the required data security standards, policies, and procedures, and has adequate security measures in place;

8.3.4 The transfer of data complies with applicable cross border transfer restrictions; and

8.3.5 A fully executed contract containing data protection clauses has been obtained and approved by the DPO and Group Legal Team.

8.4 Under certain circumstances, a Data Sharing Agreement ("DSA") may also be required.

8.5 DSAs are primarily required where multiple controllers are processing the same personal data, either

N

independently or as joint controllers.

8.6 Any sharing of personal data with third parties must be logged in The Group Sharing Register.

8.7 Any colleagues who believe that a third-party personal data transfer may be taking place without the above provisions must contact the DPO as soon as possible.

9. International Transfers

9.1 Under data protection regulations, transfers of personal data to countries outside of the UK and EEA are restricted, in order to ensure that the level of data protection afforded to individuals is not undermined.

9.2 All international transfers of personal data by The Group must be approved by the Data Protection Officer.

9.3 The Group will only transfer personal data outside of the UK/EEA if one of the following conditions applies:

9.3.1 The European Commission has issued a decision confirming that the data protection laws of the country to which the personal data is being transferred provide an adequate level of protection;

9.3.2 Appropriate safeguards are in place, such as binding corporate rules, standard contractual clauses, international data transfer agreements, an approved code of conduct, or a certification mechanism;

9.3.3 The data subject has provided informed consent for the transfer to take place; or

9.3.4 The transfer is necessary for one of the other reasons set out in the UK GDPR.

10. Personal Data Incidents

10.1 As part of the Group's obligations arising from the accountability principle, we must log and, in some circumstances, report all breaches of data protection.

10.2 A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

10.3 A near miss is an incident which does not meet the criteria of a data breach but only 'by chance'.

10.4 The Group requires all personal data breaches and near misses ("Incidents") to be reported without delay to the DPO.

10.5 The Group maintains a Personal Data Incident Procedure, which sets out the procedure to be followed upon discovery of an incident involving personal data.

10.6 Colleagues are responsible for complying with the Personal Data Incident Procedure, and failure to comply may lead to disciplinary measures.

11. Data Subject Rights

11.1 Under the UK GDPR, data subjects are afforded a set of rights with relation to the processing of their personal data.

11.2 The Group is obliged to respond to requests by data subjects for the exercise of said rights.

11.3 Such requests are referred to as Individual Rights Requests ("IRRs").

11.4 It is important that all colleagues recognise what constitutes an IRR, and how to respond to receiving such a request.

N

11.5 The Group maintains an Information Rights Request Procedure, which sets out how colleagues, and the Group as a whole, will respond to IRRs.

11.6 Colleagues are responsible for complying with the procedure set out in the Information Rights Request Procedure, and failure to comply may lead to disciplinary measures.

12. Direct Marketing

12.1 The Group is subject to rules and privacy laws with respect to direct marketing to applicants, students, alumni, and any other potential service user.

12.2 Any electronic marketing messages sent by the group (including by phone, fax, email, and text), use of website cookies, or the provision of electronic communication services to the public must be done in accordance with the Privacy and Electronic Communications Regulations 2003 ("PECR").

12.3 Any colleagues engaging in direct marketing activities are required to seek consultation and approval from the DPO prior to commencing such activities.

12.4 Consent of the data subject is generally required for any electronic direct marketing.

12.5 An exception is made for the 'soft opt-in' rule, which allows The Group to undertake direct marketing if:

12.5.1 We obtained contact details in the course of an enquiry to our services where we are marketing similar products or services;

12.5.2 We gave the individual the opportunity to opt out of marketing when first collecting their details; and

12.5.3 We give the individual the opportunity to opt out of marketing in each subsequent correspondence.

12.6 Data subjects have an absolute right to object to direct marketing, meaning that, if they do so, The Group must not continue to engage in direct marketing to the data subject under any circumstances.

12.7 If a data subject objects to direct marketing, The Group is permitted to keep sufficient personal data to ensure that we do not direct market to them again. This is known as suppression.

13. Automated Decision Making

13.1 Automated decision making is making a decision regarding an individual by purely automated means without any human involvement.

13.2 Automated decision making often includes profiling, which is the automated processing of personal data to evaluate certain things about an individual.

13.3 Under data protection regulations, The Group can only carry out automated decision making that has a significant effect on the data subject if:

13.3.1 The processing is necessary for the entry into of performance of a contract;

13.3.2 The processing is authorised by domestic law applicable to The Group; or

13.3.3 The processing is based on the data subject's explicit consent.

13.4 DPIA are required for any project involving automated decision making.

13.5 Data subject must be made aware of any automated decision making which may have a significant effect on them, and they must be given the option to have such a decision manually reviewed.

N

13.6 Information provided to data subject regarding automated decisions must contain:

13.6.1 A clear explanation of the logic involved in the decision making process;

13.6.2 An explanation of the significance of the envisaged consequences for the data subject; and

13.6.3 Information regarding the data subject's right to manual review.

13.7 Use of automated decision making must be reviewed on a regular basis, and the results of such reviews logged and sent to the DPO to be recorded.

14. Policy Governance, Review and Approval

14.1 LTE Group is registered as a Data Controller with the ICO, holding the registration reference Z8548504.

14.2 Novus Cambria are registered as a Data Controller with the ICO, holding the registration reference ZA555911.

14.3 Novus Gower are registered as a Data Controller with the ICO, holding the registration reference ZB458631.

14.4 Novus Transforming Lives Limited are registered as a Data Controller with the ICO, holding the registration reference ZB509283.

14.5 Total People Limited are registered as a Data Controller with the ICO, holding the registration reference Z1120239.

14.6 This document is proprietary to The Group. It is supplied in confidence and should not be disclosed or otherwise revealed to outside parties without prior written consent of an authorised LTE Group representative.

14.7 This group policy is approved by the Group Board and this version of the policy remains effective until it is withdrawn, or an update approved. The policy will be reviewed on an annual basis.

14.8 If any material changes are required to the policy prior to its annual review, the policy MUST be re-approved. If the changes required were insignificant (i.e. changing a job title, or department name to reflect changes in the current structure), the Accountable SMF for the policy can approve the policy, and the policy just submitted for noting to the Policy Management Framework Owner.

N

15. Information, Communication and Training

The policy will be stored on the Hub and communicated through internal communications channels as deemed appropriate. All colleagues are required to complete mandatory data protection training and confirm that they have read and understood this policy. This training must be completed by all new starters to the organisation as part of their initial mandatory training.

16. Policy Monitoring and Breaches

It is a mandatory requirement for all colleagues to fully comply with the requirements of approved LTE Group policies. Where breaches of the policy occur, they should be reported to the policy's Accountable SMF (see final section) and to the Group SHE Director.

17. Associated Policies and Documents

POLICIES	PROCEDURES & OTHER DOCUMENTS
Data Protection by Design and Default Policy	Appropriate Policy Document
Data Protection Policy	Data Protection Definitions Reference
Data Protection Impact Assessment Policy	Data Protection Impact Assessment Screening Questionnaire
Freedom of Information Act Policy	Data Protection Impact Assessment Template
Records Management Policy	Personal Data Incident Procedure
	Data Retention Schedule
	Information Rights Request Report Form
	Freedom of Information Act Procedure
	Information Asset Register
	Information Rights Request Procedure
	Information Rights Request Report Form
	Personal Data Incident Notification Letter Template
	Personal Data Incident Procedure
	Personal Data Incident Report Form

N

18. Definitions

Due to the number of terms which must be covered for the Data Protection Policy, part of this list has been moved to Appendix B of this document. The most relevant terms are defined below.

TERM	DEFINITION
Business Unit	A Distinct Business Unit within The Group, such as: Total People, MOL, Novus, UCEN, The Manchester College, Group Ops.
Colleagues	All employees, workers, contractors, agency workers, consultants, directors, members, and other individuals who work for and/or are employed by The Group.
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.
Data Controller	The person or company that is in control of the personal data. The Controller is responsible for the data and decides what to do with it in regard to processing.
Data Processor	A separate person or company who processes data on behalf of the Controller.
Data Protection Act 2018 (DPA 18)	The current UK Data Protection laws which implement the UK GDPR.
Data Protection Impact Assessment (“DPIA”)	A process designed to help a Controller or Processor systematically analyse, identify, and minimise the data protection risks of a project or plan.
Data Protection Office (“DPO”)	The Colleagues within The Group who are responsible for managing the day-to-day requirements arising from The Group’s Data Protection obligations.
Data Protection Officer	The individual responsible for managing and overseeing the data protection within an organisation.
Data Protection Regulations	The UK GDPR and Data Protection Act 2018.
Data Subject	The person to whom a given set of Personal Data refers.
General Data Protection Regulation (“GDPR”)	An EU-wide set of regulations, aimed at unifying the data protection laws of the various member stated. The GDPR is designed to allow individuals greater control over how their personal data is used, as well as protecting them from the consequences of the theft or loss of their personal data.
UK General Data Protection Regulation (“UK GDPR”)	The UK version of the GDPR, required due to the UK leaving the EU. Effectively a copy of the GDPR.
Individual Rights Request (“IRR”)	A request by a data subject to exercise one of the rights set out in the UK GDPR (covered later in this document).
Information Asset Register (“IAR”)	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’s Office (“ICO”)	The governing body responsible for upholding information rights in the UK. The ICO are responsible for enforcing many aspects of UK GDPR, including levying fines

N

	against companies in breach of the laws.
Lawful Basis	The legal justification under which a controller or processor processes personal data
LTE Group ("The Group")	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 which retains charitable status and supports national and regional government aims.
Personal Data	Any personally identifiable information relating to a Data Subject. Specifically, this can refer to the following identifiers: Name, ID number, location data, online identifier, or characteristics falling into one of these categories: physical, physiological, genetic, mental, economic, cultural, or social.
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	The processing of personal data is the handling and use, including storage and archiving, of that data.
Special Category Personal Data	Special category data is personal data that contains any of the following: Racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health information, information relating to sex life or sexual orientation, genetic, or biometric information. Additional protections are afforded to special category personal data under data protection regulations.

N

19. Version Control and Accountability

Version number	Version 3.0		
Policy Owner	Data Protection Officer		
Accountable SMF	Company Secretary & General Council/Data Protection Officer		
Approved by			
Approval Date	December 2024	**Next Review Date**	December 2026

Version	Status	Date	Revision Reason	Reviewed by	Outcome
1.0	Original Version	July 2019			
2.0	Triennial Policy Review	May 2022			
3.0	Full document review and revision.	March 2024	Document review triggered by identified need for Data Protection by Design & Default Policy.	Simon Richardson	

APPENDIX A: EQUALITY IMPACT ASSESSMENT (EIA)

Are there concerns that this policy could have an adverse impact on any of these protected characteristics?		If Yes, is action required?
Age	No	
Disability	No	
Gender reassignment	No	
Marriage or civil partnership	No	
Pregnancy and maternity	No	
Race	No	
Religion	No	
Sex	No	
Sexual orientation	No	
EIA Summary		
Person responsible for EIA	Simon Richardson – Assistant Data Protection Officer	
EIA Outcome & statement		

N

APPENDIX B: LAWFUL BASES FOR PROCESSING

B1 The Lawful bases set out in Article 6 of the UK GDPR are the legal justifications by which controllers and processors can process personal data. There are six lawful bases:

B1.1 **Consent** – The data subject has given their clear and informed consent. This has to be for a specific purpose of processing, an organisation can't gather blanket consent for all types of processing.
B1.2 **Contract** – The processing is necessary for part of a contract between the data subject and controller or processor.
B1.3 **Legal Obligation –** The processing is necessary for the organisation to comply with legal obligations. This includes things like an employer needing to pass data to a regulatory body, or processing accident reports for health and safety records.
B1.4 **Vital Interests** – The processing is necessary to protect someone's life.
B1.5 **Public Task** – The processing is necessary for the organisation to perform a task in the public interest, or for official functions. This is primarily for public sector bodies such as schools and local authorities.
B1.6 **Legitimate Interests** – Processing is necessary to the legitimate interests of the organisation. This is the least well defined of the lawful bases, and requires a formal assessment take place in order to determine whether it can be used.

B2 In addition to the above, processing of special category personal data requires that the organisation identify an addition lawful basis, as laid out in Article 9 of the UK GDPR. There are nine lawful bases for processing special category personal data:

B2.1 **Explicit Consent** – The processing is permissible if the data subject has given explicit consent for one or more specified purposes. The consent must be clear, affirmative, and documented.
B2.2 **Employment, Social Security, and Social Protection Law** – The processing is necessary for carrying out for carrying out obligations and exercising rights relating to employment, social security, and social protection law. This is typically relevant to employers and social service providers.
B2.3 **Vital Interests** – The processing is permitted if it is necessary to protect someone's life or physical wellbeing, but only where the person is unable to give consent. An example of this would relate to an emergency medical situation.
B2.4 **Not-For-Profit Activities** – Non-profit organisations can process special category personal data if it is necessary for the legitimate activities. This is only applicable if the data relates solely to members or former members, or people in regular contact with the organisation. The data also cannot be disclosed outside of the organisation without consent.
B2.5 **Manifestly Made Public** – Processing is permitted if the data has been made public by the data subject.
B2.6 **Legal Claims and Judicial Capacity** – The processing is necessary for the establishment, exercise, or defence of legal claims, or whenever courts are actin in their judicial capacity. This includes activities related to litigation and legal proceedings.
B2.7 **Substantial Public Interest** – Processing is permitted if it necessary for reasons of substantial public interest, based on UK law. This includes activities that benefit the public, unsure safety, or improve health. This basis requires that the processing be proportionate to the aim pursued and respect the essence of the right to data protection.
B2.8 **Medicine, Health, and Social Care** – Processing is permitted if it is necessary for preventative or occupational medicine, medical diagnosis, the provision of health or social care, or treatment or management of health or social care systems or services.
B2.9 **Public Health** – Processing is permitted for public health reasons, such as protecting against cross-border threats to health or ensuring high standards of quality and safety of health care and medicinal products. This processing must be supported by suitable safeguards.
B2.10 **Scientific, Historical, or Statistical Purposes** – Processing is permitted if it is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes. This processing is subject to appropriate safeguards to ensure the rights and freedoms of the data subjects involved.

N

APPENDIX C: FULL TERMS LIST

TERM	DEFINITION
Anonymisation	The process of altering personal data such that it is no longer identified or identifiable, meaning that it is no longer considered personal data.
Automated Decision-Making	Where a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects on 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 within The Group, such as: Total People, MOL, Novus, UCEN, The Manchester College, Group Ops.
Colleagues	All employees, workers, contractors, agency workers, consultants, directors, members, and other individuals who work for and/or are employed by The Group.
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.
Compliance Risks	Risks which affect The Group, such as a breach of the data protection regulations, potentially leading to regulatory action, a fine, or reputational damage.
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.
Data Controller	The person or company that is in control of the personal data. The Controller is responsible for the data and decides what to do with it in regard to processing.
Data Controllers in Common	Two or more controllers sharing a pool of personal data which they both process separately.
Data Processor	A separate person or company who processes data on behalf of the Controller.
Data Protection by Design and Default (“DPbDD”)	The principle that organisations should ‘bake in’ data protection to all processing activities and business practices.
Data Processing Agreement	A formal agreement between a controller and processor, setting out how the processor is expected to treat the personal data that the controller shares with them. Legally required when a controller processor relationship exists.
Data Protection Act 2018 (DPA 18)	The current UK Data Protection laws which implement the UK GDPR.
Data Protection Impact Assessment (“DPIA”)	A process designed to help a Controller or Processor systematically analyse, identify, and minimise the data protection risks of a project or plan.
Data Protection Office (“DPO”)	The Colleagues within The Group who are responsible for managing the day-to-day requirements arising from The Group’s Data Protection obligations.
Data Protection Officer	The individual responsible for managing and overseeing the data protection within

N

	an organisation.
Data Protection Regulations	The UK GDPR and Data Protection Act 2018.
Data Sharing Agreement (“DSA”)	A document setting out a common set of rules to be followed by two or more organisations who are sharing personal data. It contains the purpose of the data sharing, the data being shared, the organisations involved, as well as other information regarding how data should be handled. DSAs tend to be needed where multiple controllers are working with the same personal data, either independently or as joint controllers.
Data Sharing and Contracts Register	A register containing an overview of organisations with whom we share Personal Data. The Register contains the categories of Personal Data, Lawful Basis, Contract Lead, etc.
Data Subject	The person to whom a given set of Personal Data refers.
Direct Marketing	The communication (by whatever means) of any advertising or marketing material which is directed to particular individuals.
General Data Protection Regulation (“GDPR”)	An EU-wide set of regulations, aimed at unifying the data protection laws of the various member stated. The GDPR is designed to allow individuals greater control over how their personal data is used, as well as protecting them from the consequences of the theft or loss of their personal data.
UK General Data Protection Regulation (“UK GDPR”)	The UK version of the GDPR, required due to the UK leaving the EU. Effectively a copy of the GDPR.
Incorrect Recipient	An individual or organisation to whom personal data has been sent in error.
Individual Rights Request (“IRR”)	A request by a data subject to exercise one of the rights set out in the UK GDPR (covered later in this document).
Information Asset Register (“IAR”)	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’s Office (“ICO”)	The governing body responsible for upholding information rights in the UK. The ICO are responsible for enforcing many aspects of UK GDPR, including levying fines against companies in breach of the laws.
Joint Controller	Two or more controllers acting together to decide the purposes and manner of processing of a given set of personal data. There are specific parts of the UK GDPR which apply to joint controllers. This is distinct from controllers in common.
Lawful Basis	The legal justification under which a controller or processor processes personal data
LTE Group (“The Group”)	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 which retains charitable status and supports national and regional government aims.
Personal Data	Any personally identifiable information relating to a Data Subject. Specifically, this can refer to the following identifiers: Name, ID number, location data, online

N

	identifier, or characteristics falling into one of these categories: physical, physiological, genetic, mental, economic, cultural, or social.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.
Privacy Enhancing Technologies ("PETs")	Software and hardware technologies that embody the data protection principles by minimising personal data use, maximising data security, or empowering data subjects.
Processing	The processing of personal data is the handling and use, including storage and archiving, of that data.
Pseudonymisation	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.
Risk	The potential for harm to Data Subjects arising from a given Processing activity. This can include physical, material, and non-material (e.g. distress) harm.
Special Category Personal Data	Special category data is personal data that contains any of the following: Racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health information, information relating to sex life or sexual orientation, genetic, or biometric information. Additional protections are afforded to special category personal data under data protection regulations.
Subject Access Request ("SAR")	A request made by a data subject to a controller or processor for a copy of all the data that they hold on the data subject.
Suppression	The practice of, instead of deleting an individual's details entirely, 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.

N