CENTRE AGREEMENT - TERMS AND CONDITIONS

APPENDIX 3 – DATA SHARING AGREEMENT

1. Status

1.1 Each Party shall be an independent Controller of the Shared Personal Data under Data Protection Law.

1.2 A Party can be either a Data Discloser or a Data Receiver in respect of the Shared Personal Data and references in this Agreement to "**Data Discloser**" or "**Data Receiver**" shall be construed according to the particular Party that is sharing the relevant Shared Personal Data at the relevant time.

1.3 This Agreement allocates certain rights and responsibilities amongst the Parties as enforceable contractual obligations between themselves, however nothing in this Agreement is intended to mean that a Party is not required to meet its own responsibilities under Data Protection Law. Each Party warrants that it will (and will ensure that its Workforce and sub-processors will) comply with the Data Protection Law in relation to the Shared Personal Data.

2. Purpose

2.1 This Agreement sets out the framework for the sharing of Personal Data when the Data Discloser discloses personal data to the Data Receiver. It defines the principles and procedures that the Parties shall adhere to and the responsibilities the Parties owe to each other and to the Data Subjects.

2.2 The Parties agree that this Appendix 3 relates to the ongoing and routine sharing of the Shared Personal Data for the Agreed Purpose during the Term.

2.3 The type of Personal Data processed pursuant to this Agreement and the subject matter, duration, nature and purpose of the processing, and the categories of Data Subject, are described in Appendix 3, Schedule 1 (Particulars of the Shared Personal Data).

2.4 The Parties have determined that it is necessary to share the Shared Personal Data and the Data Receiver agrees to only process Shared Personal Data for the Agreed Purpose and not to process Shared Personal Data in a way that is incompatible with the Agreed Purpose, except with the prior written agreement of the Data Discloser.

2.5 Each Party shall appoint at least one Contact Point with responsibility for any issues arising from the sharing and processing of the Shared Personal Data and for actively improving the effectiveness of the sharing and processing. The Contact Point must be an individual associated with the respective organisation with sufficient knowledge and experience of Data Protection Law so as to be able to take decisions on behalf of that Party in relation to data protection and privacy matters.

2.6 Each Party may update its Contact Point by written notice to the other Party.

3. Compliance

3.1 Subject to Paragraph 3.3 below, each Party shall at all times comply with all applicable Data Protection Law in connection with the exercise and performance of its respective rights and obligations under this Agreement.

3.2 In the event that the Data Protection Law applicable to you (including any Data Protection Law applicable in the Territory) conflicts with the Data Protection Law applicable in the UK, you shall apply the Data Protection Law that necessitates stricter or additional requirements to protect Data Subjects' privacy and Personal Data whilst ensuring that you remain compliant with Data Protection Law applicable in the UK and you shall promptly notify Ascentis of any such conflict and advise Ascentis of the steps you have taken to ensure such compliance.

3.3 Notwithstanding anything else contained in this Agreement, you shall use your best endeavours to assist Ascentis with complying with its obligations under Data Protection Law and you shall not perform your obligations under this Agreement in such a way as to cause Ascentis to breach any of its obligations under Data Protection Law.

3.4 Each Party warrants that it has such valid registrations and has paid such fees as are required by their applicable Supervisory Authorities which, by the time that the sharing of the Shared Personal Data is expected to commence, cover the intended sharing of Personal Data pursuant to this Agreement.

3.5 If Data Protection Law in any applicable jurisdiction (including the Territory) requires the obligations in this Agreement to be supplemented by additional or alternative provisions, the Parties shall work together, at your cost, to ensure that that those provisions are enacted.

3.6 Each Party will promptly notify the other Party (within at least two (2) working days) if it receives a complaint or request relating to the other Party's obligations under Data Protection Law (other than a Data Subject Request, which is addressed in Paragraph 9 (Dealing with data subject requests) below). On receipt of such a notice, the notifying Party will provide the other Party with reasonable co-operation and assistance in relation to any such complaint or request.

4. General obligations

4.1 Each Party will process the Shared Personal Data in accordance with the Particulars set out in Appendix 3, Schedule 1 (Particulars of the Shared Personal Data).

4.2 The Shared Personal Data must not be irrelevant or excessive with regard to the Agreed Purpose and the Data Discloser shall ensure that the Shared Personal Data has been collected, processed, and transferred in accordance with Data Protection Law at all times prior to the receipt of that Personal Data by the Data Receiver.

4.3 You are responsible for ensuring that, where the Shared Personal Data was received from a third party, you have in place an agreement with that third party which is adequate to permit you to share the Shared Personal Data with Ascentis in accordance with Data Protection Law, and you shall promptly provide English copies of any such agreement to Ascentis on request of Ascentis.

4.4 You will complete a data protection impact assessment if required under Data Protection Law and you will provide Ascentis with all reasonable assistance it requests in relation to completing its own data protection impact assessment in respect of the planned sharing of the Shared Personal Data under this Agreement.

5. International data transfers

5.1 It is acknowledged and understood that the sharing of the Shared Personal Data between the Parties under this Agreement may necessitate the transfer of the Shared Personal Data:

5.1.1 from the United Kingdom to the EEA and non-EEA countries ("**UK Restricted Transfers**"); and

5.1.2 from the EEA to non-EEA countries ("**EEA Restricted Transfers**"),

(together, the "**Restricted Transfers**").

5.2 If a Party intends to carry out an EEA Restricted Transfer and the transfer is not to an Adequate Country, the EU Model Clauses will apply to such EEA Restricted Transfer, with the Party based outside the EEA acting as a Data Importer and the Party based inside the EEA acting as a Data Exporter. The Parties will comply with the EU Model Clauses as detailed in Appendix 3, Schedule 2 and its Annexes, and take all other actions required to ensure that the transfer is made in accordance with Data Protection Law.

5.3 If a Party intends to carry out a UK Restricted Transfer and the transfer is not to an Adequate Country, the UK Addendum will apply to the UK Restricted Transfer, with the Party based outside the UK acting as a Data Importer and the Party based inside the UK acting as a Data Exporter. The Parties will comply with the UK Addendum as detailed in Appendix 3, Schedule 3 and its Annexes, and take all other actions required to ensure that the transfer is made in accordance with Data Protection Law.

5.4 If either of the Model Clauses are updated by the European Commission or UK Government (as relevant), the Parties shall promptly enter into an amended form of the Model Clauses as required, unless the Parties agree that another mechanism under Data Protection Law can be relied upon to provide adequate protection to the Shared Personal Data.

5.5 If the Parties have not agreed that another mechanism under Data Protection Law can be relied upon to provide adequate protection to Shared Personal Data by the time the amended Model Clauses are in force, and either Party refuses to and/or otherwise does not enter into an amended form of the Model Clauses in accordance with Paragraph 5.4, the other Party reserves the right to terminate this Agreement with immediate effect.

5.6 If the Model Clauses cease to be valid, whether by a decision of a court of competent jurisdiction, the European Commission or the UK Government (as relevant), the Parties will co-operate in good faith to ensure that any continued Restricted Transfers are compliant with Data Protection Law.

5.7 For the avoidance of doubt, in the event of any conflict between the Model Clauses and the clauses in the rest of this Agreement, the Model Clauses shall take precedence.

6. Lawful, fair, and transparent processing

6.1 Each Party shall ensure that it processes the Shared Personal Data fairly and lawfully in accordance with Paragraph 6.2 during the Term.

6.2 Each Party shall ensure that it has a Lawful Basis under Data Protection Law for the transfer and Processing of Shared Personal Data and, where the Lawful Basis relied on is Consent, will ensure that evidence of the Data Subject's Consent is available to the Data Receiver.

6.3 You warrant that you have verified that any Consent obtained by you or on your behalf in relation to the Shared Personal Data is sufficient for the purposes of your own and Ascentis'

processing activities under this Agreement and that effective procedures are in place to allow the Data Subject to "withdraw" their Consent in line with Data Protection Law.

6.4 If you become aware that any Consent is withdrawn by the Data Subject or if a relevant Data Subject has requested that their Shared Personal Data is no longer processed for all or any particular purposes, you shall promptly notify Ascentis of this.

6.5 You shall, in respect of the Shared Personal Data, ensure that you provide a Privacy Notice to the Data Subjects, in accordance with Data Protection Law, containing clear and sufficient information about the purposes for which you will Process their Personal Data, the Lawful Basis for such Processing and such other information as is required by Data Protection Law, including:

6.5.1 that their Personal Data will be shared with Ascentis, which must be identified in your applicable Privacy Notice, along with sufficient information about such sharing and the purpose of such sharing to enable the Data Subject to understand the purpose and risks of such sharing;

6.5.2 if Shared Personal Data will be transferred to a third party, that fact, and sufficient information about such transfer and the purpose of such transfer to enable the Data Subject to understand the purpose and risks of such transfer; and

6.5.3 whether Shared Personal Data will be transferred outside the Territory and/or the United Kingdom (as applicable), with sufficient information about such transfer, the purpose of such transfer and the safeguards put in place by the Controller, to enable the Data Subject to understand the purpose and risks of such transfer.

6.6 Ascentis undertakes to inform the Data Subjects, to the extent that it is required to do so under Data Protection Law, of the purposes for which it will process their Personal Data, the lawful basis for such purposes and any other information as is required by Data Protection Law.

7. Data accuracy and quality

7.1 The Parties agree to (i) use compatible datasets to record all Shared Personal Data; or (ii) develop a reliable means of converting Shared Personal Data to ensure compatibility with each Party's respective datasets. The Parties shall reconcile the Shared Personal Data into a consistent and complete view that can be disclosed to Data Subjects on request.

7.2 The Data Discloser will ensure that the Shared Personal Data is accurate and up to date when disclosed or made accessible to the Data Receiver and shall promptly notify the Data Receiver if such Shared Personal Data becomes inaccurate or out of date during the Term (together with revised and corrected data).

7.3 Without prejudice to any other obligation, if either Party becomes aware that any of the Shared Personal Data is inaccurate or out of date, it shall promptly notify the other of such.

8. Records

8.1 Each Party shall maintain complete, accurate and up to date written records of all of its processing of the Shared Personal Data and as necessary to demonstrate its compliance with this Agreement and Data Protection Law.

9. Dealing with data subject requests

9.1 Each Party will ensure that it protects the rights of Data Subjects under Data Protection Law and agrees to promptly notify the other Party in writing (within at least two (2) working days) if it receives a Data Subject Request in relation to the Shared Personal Data.

9.2 Each Party agrees that the Data Subject Request will be dealt with by the Party in receipt of the Data Subject Request, and that the other Party will provide all reasonable co-operation and assistance in relation to any Data Subject Request to enable the Party in receipt of the Data Subject Request to comply with the Data Subject Request within the relevant timescale set out in Data Protection Law.

9.3 Each Party in receipt of a Data Subject Request will ensure it responds to any such Data Subject Request adequately and in accordance with Data Protection Law.

9.4 Each Party in receipt of a Data Subject Request will notify the other Party of the Data Subject Request received and will keep the other Party updated as to the progress and resolution of the Data Subject Request.

9.5 You shall indemnify and hold Ascentis harmless from any cost, charge, damages, expense, or loss which you cause Ascentis as a result of your breach of any of the provisions of this Paragraph 9.

10. Data retention and deletion

10.1 Except as required by Relevant Legislation and subject to Paragraph 10.2, the Data Receiver shall:

10.1.1 process the Shared Personal Data for no longer than such processing is necessary for the Agreed Purpose and in compliance with this Agreement and Data Protection Law;

10.1.2 cease to process all Shared Personal Data, and ensure that it is returned to the Data Discloser or destroyed in accordance with the agreed Deletion Procedure set out in Paragraph 11 (Data deletion), on the earlier of termination or expiry of this Agreement; and

10.1.3 immediately, confidentially, and securely destroy or dispose of all Shared Personal Data (and all copies) in its possession or control that is no longer necessary for the Agreed Purpose or can no longer be processed in accordance with this Agreement.

10.2 Notwithstanding Paragraph 10.1, the Parties shall continue to retain Shared Personal Data in accordance with any applicable statutory or professional retention periods or where the Personal Data forms part of the certification provided by Ascentis.

10.3 Following the deletion of Shared Personal Data in accordance with Paragraph 10.1, the Data Receiver shall notify the Data Discloser that the Shared Personal Data in question has been deleted in accordance with the Deletion Procedure in Paragraph 11 (Data deletion).

11. Data Deletion

11.1 The Parties shall take the Storage Limitation Principle into account and balance it against their requirements to retain the Shared Personal Data and each warrant that they have deletion procedures and data policies in place which adhere to Data Protection Law and shall make such documents available to the other Party on request.

11.2 If the Data Discloser advises the Data Receiver that Shared Personal data must be deleted, then the Data Receiver shall:

11.2.1 promptly remove or make inaccessible, that part of the Shared Personal Data from their systems or any offsite storage or third-party facilities and return to other Party or Data Subject (as relevant) and/or destroy the Shared Personal Data subject to the request for return and/or deletion within a reasonable timeframe, but after the termination of the applicable legal data retention periods or valid deletion request;

11.2.2 ensure all media used solely to store the relevant Shared Personal Data will be returned to the other Party and/or Data Subject (as applicable) and/or destroyed in a secure manner or have the client Data permanently and irrevocably removed; and

11.2.3 provide a written certification regarding such removal and/or destruction within thirty (30) calendar days of such occurrence.

11.3 Any deletion/destruction of Shared Personal Data must stop immediately upon notification from a Party that preservation of documents for contemplated litigation is required (sometimes referred to as a litigation hold). Destruction may begin again once that Party lifts the requirement for preservation.

12. Security and training

12.1 The Parties undertake to have in place throughout the Term appropriate technical and organisational security measures to:

12.1.1 prevent:

12.1.1.1 unauthorised or unlawful processing of the Shared Personal Data; and

12.1.1.2 the accidental loss or destruction of, or damage to, the Shared Personal Data

12.1.2 ensure a level of security appropriate to:

12.1.2.1 the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction, or damage; and

12.1.2.2 the nature of the Shared Personal Data to be protected.

12.2 The level of technical and organisational measures agreed by the Parties, as appropriate as at the Commencement Date having regard to the state of technological development and the cost of implementing such measures, is set out below. The Parties shall keep such security measures under review and shall carry out such updates as they agree are appropriate throughout the Term.

12.3 Where the Data Discloser shares Shared Personal Data, it will provide the Shared Personal Data in in a manner consistent with Paragraphs 12.4 and 12.5.

12.4 Data Security Measures

12.4.1 The Data Discloser shall ensure the Shared Personal Data is transferred to the Data Receiver using appropriate security measures, such as pseudonymisation and specific encryption methods, as set out in Article 32(1) of the UK GDPR.

12.4.2 Each Party shall, to the extent it is the Data Receiver, implement and maintain the following measures in respect of received Shared Personal Data:

Ascentis

12.4.2.1 Encryption methods where applicable – in transit (i.e., email); and end to end for all projects from (platforms; API; automated)

12.4.2.2 Anonymisation/Pseudonymisation where possible and applicable

12.4.2.3 Cyber Essential standards

You:

12.4.2.4 Encryption methods where applicable – in transit (i.e., email); and end to end for all projects from (platforms; API; automated)

12.4.2.5 Anonymisation/Pseudonymisation where possible and applicable

12.5 Workforce

12.5.1 Each Party shall, to the extent it is the Data Receiver, at all times ensure the processing of the Shared Personal Data by natural persons shall be limited to its Workforce (and the Workforce of its sub-contractors subject to any approvals required under this Agreement) that need to process it for the Agreed Purpose in accordance with this Agreement.

12.5.2 It is the responsibility of each Party to ensure that its Workforce are appropriately trained to handle and process the Shared Personal Data in accordance with the technical and organisational security measures set out in this Paragraph 12 together with any other applicable Data Protection Law and guidance and that it has entered into appropriate confidentiality agreements relating to the processing of Shared Personal Data.

12.5.3 The level, content and regularity of training referred to in Paragraph 12.5.2 shall be proportionate to a Workforce members' role, responsibility, and frequency with respect to their handling and processing of the Shared Personal Data.

13. Personal data breaches and reporting procedures

13.1 Each Party shall comply with its obligation to report a Personal Data Breach to the ICO or appropriate Supervisory Authority and (where applicable) Data Subjects, and shall each inform the other Party of any Personal Data Breach in accordance with this Paragraph 13, irrespective of whether there is a requirement to notify the ICO, any Supervisory Authority or Data Subjects.

13.2 Each Party warrants that it has a suitable Personal Data Breach response plan in place which adheres to Data Protection Law and shall make such documents, as far as they relate to the Shared Personal Data and this Agreement, available to the other Party on request.

13.3 A Party shall promptly (and in any event within 24 hours) notify the other Party if it suspects or becomes aware of any actual or threatened occurrence of any Personal Data Breach in respect of any Shared Personal Data. Such notifications will (as far as reasonably possible) include a full description of:

13.3.1 the nature of the Personal Data Breach including details of the Shared Personal Data and Data Subjects affected;

13.3.2 the likely consequences of the Personal Data Breach; and

13.3.3 the measures taken or proposed to be taken by the Breached Party to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

13.4 The other Party's obligations under this Paragraph 13 shall be performed at the Breached Party's reasonable expense, except to the extent that the Personal Data Breach (or the circumstances giving rise to the Personal Data Breach, or it being threatened or suspected) arose out of any negligence or wilful default of the other Party or any breach by the other Party of its obligations under this Agreement, in which case the costs shall be borne at the other Party's cost and expense.

13.5 The Parties agree to provide reasonable assistance as is necessary to each other to facilitate the handling of any Personal Data Breach in an expeditious and compliant manner, including:

13.5.1 making available all relevant data and records required for either Party to comply with Data Protection Law or as otherwise reasonably required by the Breached Party,

13.5.2 taking such reasonable steps as are directed by the Breached Party to assist in the investigation, mitigation, and remediation of a Personal Data Breach (which may include providing the Breached Party with physical access to any facilities affected and facilitating the interview of staff and others involved in the matter);

13.5.3 providing reasonable assistance to the other Party in the event that such Party is required to notify a relevant Supervisory Authority, other regulator and/or affected Data Subjects; and

13.5.4 co-ordination regarding the management of public relations and public statements relating to the Personal Data Breach.

13.6 The Breached Party will provide regular updates to other Party on the progress of its investigation into the Personal Data Breach.

14. Resolution of disputes with Data Subjects or Supervisory Authorities

14.1 In the event of a dispute or claim brought by a Data Subject, ICO or another applicable Supervisory Authority concerning the processing of Shared Personal Data against either or both Parties, the Parties will inform each other about any such disputes or claims without delay and will cooperate with a view to settling them amicably in a timely fashion.

14.2 Where it is reasonably practicable to do so, the Parties agree to:

14.2.1 respond to any generally available non-binding mediation procedure initiated by a Data Subject, the ICO or applicable Supervisory Authority; and

14.2.2 consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

15. Indemnity

15.1 Subject to Paragraph 15.2, the Data Discloser and Data Receiver undertake to indemnify each other and hold each other harmless from any cost, charge, damages, expense, or loss which they cause each other as a result of their breach of any of the provisions of this Agreement, except to the extent that any such liability is excluded under this Agreement or Relevant Legislation.

15.2 You will inform and advise Ascentis of any requirements or obligations Ascentis has under Data Protection Law. You shall indemnify, protect, defend and hold harmless Ascentis from any and all liabilities, obligations, losses, damages, penalties, actions, judgments, suits, claims, costs, expenses and disbursements of any kind or nature whatsoever (including, without limitation, the reasonable fees and disbursements of counsel) whether direct, indirect or consequential and whether based on any local or foreign laws, statutes, rules or regulations, in any manner relating to or arising out of a result of your breach of Data Protection Law or your failure to inform Ascentis of any requirements or obligations that Ascentis may have under Data Protection Law.

16. Changes to Data Protection Law

16.1 If, during the Term, Data Protection Law changes in such a way that relevant provisions in the Centre Agreement (including this Appendix 3) are no longer adequate or appropriate for compliance with Data Protection Law, the Parties agree that they will negotiate in good faith, at your cost, to review and update those relevant provisions in the light of the new Data Protection Law.

SCHEDULE 1 – PARTICULARS OF THE SHARED PERSONAL DATA

1. Categories of Data Subjects

- Learners
- Staff of other party

2. Categories of Personal Data

- Student full name
- Student DOB
- Student gender
- Student identification number
- Student school email address
- Student post code
- Unique Learner Number (ULN)
- Student assessed work and achievement record
- Staff full name
- Staff job titles
- Staff business email addresses
- Staff CVs including home address, personal email, and personal phone numbers where staff have included these in CVs which they have provided to the College
- Evidence of qualifications that [Centre name] provides
    - Delivered through other AOs (Awarding Organisations)
    - Delivered by Ascentis

3. Sensitive Data – Special Category Data:

- Record of any extenuating circumstances
- Reasonable adjustment / Special Consideration
- Student ethnicity
- Learning difficulties and disability

As this can include information relating to an individual's physical/mental health, the upmost care will be taken during processing.

4. Sensitive Data – Criminal Offence Data

Criminal Offence Data will not be shared between the parties unless required by law.

5. Applied restrictions or safeguards in relation to Sensitive Data

The Parties will ensure that there are strict measures in place to protect the sensitive data listed in paragraphs 3 and 4 above. These safeguards include:

- Encryption: Encrypting sensitive data both in transit and at rest to prevent unauthorised access.
- Access Controls: Implementing role-based access controls to limit who can access sensitive data.
- Data Minimalization: Collecting and retaining only the minimum necessary sensitive data.
- Regular Audits: Conducting periodic security audits to identify and rectify vulnerabilities.
- Data Protection Impact Assessments (DPIAs): Assessing the impact of data processing activities on individuals' privacy and implementing necessary mitigations.

6. Frequency of the transfer of Personal Data

The frequency of transferring personal data will depend on the specific activities that are being undertaken. Common scenarios might include:

- Regular data transfers for processing certificates or qualifications.
- Transfers for enrolment or registration.
- Ad hoc transfers for resolving issues or inquiries.

The frequency will also depend on our policies and legal requirements, such as data subject consent and data protection regulations.

7. Nature of the Processing

The nature of data processing can vary widely, including, but not limited to:

- Registration and enrolment processes.
- Assessment and examination procedures.
- Certificate or qualification issuance.
- Customer support and inquiry handling.

Each of these processes may involve different types of personal data and may require specific data processing activities.

8. Purpose(s) of the transfer of Personal Data and further Processing

The purposes for which we transfer and process personal data may include, but is not limited to:

- To verify and record students' identities and qualifications.
- To issue certificates or qualifications.
- To provide support and respond to inquiries.
- To meet legal or regulatory requirements.
- To conduct research or analysis for educational improvement.

The Parties will ensure that personal data is processed only for the purposes for which it was collected, and individuals are informed about these purposes through privacy notices or policies.

9. Retention period or criteria

No personal information will be kept by a Party longer than is necessary to perform that Party's obligations under the Centre Agreement.