INVICTUS
Education Trust

INVICTUS EDUCATION TRUST

OUTSOURCING POLICY

Approved by Board of Trustees
25 May 2021

To be reviewed by Board of Trustees
April 2023

Document Provenance

Outsourcing Policy	
Committee Approval Level	Board of Trustees
Policy Author/Responsibility	Chief Operating Officer – Julie Duern
Policy First Implemented	July 2018
Frequency of Review	Every 2 Years
Next Review Date	April 2021
Policy Approved by Committee	25 May 2021
Next Review Date	April 2023

CONTENTS **PAGE**

1. Policy Statement

Invictus Education Trust outsources various operational functions to third parties, where there is an educational/business need or where the outsourcing of such functions is a legal, statutory, contractual or regulatory requirement. In doing so, we understand that additional risk can be posed to both business and customer, and as such we are committed to ensuring the continued quality, high standards and compliance of any outsourced process.

Where any task or activity is outsourced, the Trust employs structured and robust assessments, due diligence and monitoring measures and procedures, both prior to entering into any supplier contract and for the duration of the business relationship. Our dedicated procedures are used to initiate, maintain and monitor the operational function of the outsourced process as well as in assessing the expertise, quality and ongoing compliance of the supplier or vendor.

The Trust is committed to providing a professional, reliable and transparent service and we are committed to verifying that any third-party service provider(s) are suitable, competent and trustworthy prior to forming any business relationship.

2. Purpose

The purpose of this policy is to provide the Trust's statement of intent and objectives for how we manage and monitor our outsourced business processes and the supplier carrying out those functions. It also provides systematic procedures and guidance for staff and associated entities concerning the Trust's processes and methodology for outsourcing.

The Trust has set appropriate and adequate objectives to enable us to meet our legal, regulatory and ethical obligations for outsourced processes and to enable our staff to identify, manage and mitigate any associated financial, operational and business risks. We only ever use those providers whom we have vetted and verified as being compliant, competent, suitable and reliable and we ensure the continued provision of such attributes through due diligence checks and ongoing monitoring.

3. Scope

The policy applies to all staff *(meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with the Trust) w*ithin the organisation and has been created to ensure that staff deal with the area that this policy relates to in accordance with legal, regulatory, contractual and business expectations and requirements.

4. What is Outsourcing?

For the purposes of this document*, 'outsourcing'* refers to any business function or service that is, provided by, or contracted out, to an external, non-associated provider or supplier. Examples of commonly outsourced functions include alternative education providers, professional consultants, payroll, HR, insurance etc.

Outsourcing usually happens for three reasons:

- The Trust is unable to complete a function or service in-house, possibly due to constraints on resources, time, space or the skill level needed to complete the task
- It is more cost effective to outsource certain functions or processes
- There is a legal or regulatory requirement for outsourcing

Where the Trust outsources any of its educational/business functions, it has a duty to its student, parents, staff, customers and regulators to ensure that the function is still being completed compliantly, ethically and satisfactorily. It is ultimately the Trust's responsibility to ensure compliance, even when the function or process is being completed elsewhere, which is why strict and robust outsourcing policy and procedures documents are necessary.

5. Objectives

The Trust confirms that in relation to outsourced educational/business services or processes and when using the services of third parties, service providers or processors, we ensure that the below objectives are met through implementing procedures, systems and controls.

Invictus Education Trust agrees to:

- avoid any undue operational risks when relying on a service provider for all or part of an operational function
- not to outsource any important operational risk that may impair the quality of the Trust's internal control or the regulators ability to monitor the firm's compliance with our obligations under the regulatory and legal system
- implement policies and procedures which govern the use of outsourcing and any service provider used
- carry our frequent and rolling audits *(physical and remote)* on any service provider in relation to their conduct, ability to perform the outsourced task and required compliance
- ensure that the service provider has the correct ability, capacity and any required authorisation to carry out the required function
- ensure that the service provider protects any sensitive and/or confidential information supplied to them in the course to the business relationship
- identify and implement disaster recovery and business continuity procedures and contingencies for any service or function that has been outsourced and to carry out periodic reviews and tests of any such plans
- ensure that a Contract or Service Level Agreement (SLA) is in place and agreed to by both the Trust and service provider, prior to any business relationship forming
- carry out a due diligence check and assessment prior to signing the contract.
- ensure that no outsourcing arrangement diminishes our ability to meet our contractual, regulatory and compliance obligations
- evaluate all risks associated with the outsourcing functions to ensure viability of implementation
- ensure the providers ability to maintain the privacy, security, and data protection obligations as applicable to our Trust.

- enforce and monitor that all third parties used for outsourcing or as contractors, lead generators or introducers, comply with and agree to follow this Outsourcing Policy & Procedure and the obligations and procedures contained herein as well as accepting our Due Diligence checks, ongoing monitoring and evaluation and selection procedures

6. Risk Assessment

Prior to outsourcing any educational/business service or function, the Trust identifies any educational/operational, financial and/or business risks that may present themselves by using an external provider or outsourcing a specific service or process. These risks are assessed using a Risk Matrix and assigned an impact/probability rating which forms part of the Trust's decision on whether to proceed.

Other risks that can be associated with outsourcing are:

- Financial
- Reputation
- Service/Product Quality
- Delays
- Timeframes
- Rights of individuals
- Ability to comply with regulatory requirements
- Due Diligence

The Trust uses a comprehensive due diligence checklist/tender specification to ensure that any service provider considered for an educational/business relationship is fit for purpose, reliable, suitable, competent, qualified and experienced.

In addition to the questions and assessment, areas contained in our due diligence checks; the selection of providers for outsourced services is also based on the following criteria:

- Length of experience and depth of expertise in the services and/or functions being offered
- Obtaining samples and evidence of any similar previous work carried out
- Obtaining references or testimonials from previous and/or existing clients
- Cost analysis of services and/or processes provided
- Contractual arrangements consistent with this Outsourcing Policy and Procedures

7. Procedures

7.1 Assessment & Analysis

Prior to any outsourcing agreement being made, the below procedures must be followed and recorded for each new relationship.

- The services/functions being considered for outsourcing is assessed to see if it is a general educational/business activity, or involves all or part of a regulated activity or the processing of personal data. Where the service/function to be outsourced does involve processing personal information, the Trust:

    - assesses and monitors the service providers (*processors*) compliance with the GDPR
    - has a principle contract and processor agreement in place covering the obligations and responsibilities of the processor during the business relationship
    - carries out a risk assessment and ongoing audits to verify the existence and use of the required operational and technical measures for security of processing

- An *'outsource risk/benefit analysis assessment'* is completed for the function/service under consideration, which must include the below information:

    - Possible efficiency/monetary/quality gains by outsourcing the service
    - List of detailed risks associated with outsourcing the service
    - List of defined benefits and downsides to outsourcing the service
    - Departments and/or staff who will be affected by/involved in the outsourced function
    - Arrangement for monitoring the quality and compliance of the outsourced functions and supplier
    - Scope and timeframe for outsourcing the process or service
    - Internal staff changes, and additional training needed in relation to the outsourcing
    - Implementation of any new systems

7.2 Preparation & Selection

After the initial decision to proceed with outsourcing has been made, the Trust creates a criteria list to be used in the selection stage of the outsourcing process. The criteria list is specific to each project and details the objectives, obligations, standards and requirements that must be met by the supplier.

We then collate a list of suitable vendors who can be considered as the outsourced function provider. This list is compiled using vendors in the market who are suitable to provide the outsourced function. This list is usually large in the first instance but is narrowed down through the tendering, assessment process, and the project requirements. We collect written information about the capabilities of various suppliers so that the information provided can be assessed against our selection criteria, and used for comparative purposes.

The tendering process will include specific details about the scope and requirements of the project to ensure that vendors can respond to and price accordingly. Such information includes, but is not limited to:

- Scope of opportunity
- Relevant requirements and objectives
- Timescales and project length
- Staff & training requirements
- Educational/Industry requirements
- Regulatory requirements
- Systems, technology and/or governance requirements
- SLA and/or Contract specifics
- Volume of data *(where applicable)* or job size
- Ongoing monitoring & due diligence
- Outcomes and performance

The tender document is then distributed to all participating vendors with specific information on the engagement requirements timelines for questions and responses and key information.

7.3 Evaluation

Once all completed tenders have been received, we enter the evaluation stage of the outsourcing process and short list potentially successful vendors. Vendors who are discounted at this stage are contacted in writing within 4 weeks and provided with a summary of why they have been unsuccessful in bidding for this project. Once a successful vendor is selected and approved by Board, we can start the change management processes of the selected vendor.

7.4 Allocation & Due Diligence

A due diligence audit and questionnaire is completed for the successful vendor prior to any agreement being entered into. The Trust will ensure that it considers:

- Vendor's reputation and history
- quality of services provided to other customers
- number and competence of staff and managers
- financial stability of the company and commercial record
- retention rates of the company's employee
- company's adherence to relevant regulatory requirements and laws
- compliance with the GDPR and the presence of mandatory operational and technical measures for secure processing and data subject rights
- A detailed company check, and background search must be completed on the service provider and prior to any agreement being made
- A physical visit to the providers' services location must be made with a view to carrying out a physical on-site audit

7.5 Outsourcing Agreement

The agreement will address the below areas, and signed by both parties, at the commencement of the service:

- Duties and obligations of the Trust
- Duties and obligations of the service provider
- Applicable law to outsourcing agreement
- Regulations that apply to the outsourced service/function
- Duration of the Agreement
- Terms of the Agreement
- Reporting
- Audits & Monitoring
- Dispute Resolution
- Confidentiality Agreement
- Non-Compete Agreement
- Appeal & Enforcement

7.6 Third-Party Processors

Where the Trust utilise external processors for carrying out certain personal data processing activities, we have specific obligations under the data protection laws to ensure that such providers are compliant with the GDPR and have the rights of the individuals in mind when processing. We use information audits to identify, categorise and record all personal data that is processed outside of the Trust, so that the information, processing activity, processor and legal basis are all recorded, reviewed and easily accessible. Such external processing includes *(but not limited to):*

- School Admission Services
- Alternative Education Services
- Counselling Services
- Careers Advisor Services
- Education Welfare Services
- Learning Support Services
- Music Services

- Catering Services
- Payroll Services
- HR Services
- Legal Services
- Insurance Services
- Audit Services
- Health & Safety Services
- Specialist Educational Consultant Services

Invictus Education Trust has a dedicated Processor Agreement (Appendix 1) which is used for all outsourced functions relating to personal information, and obtains company documents, certifications, references and ensure that the processor is adequate, appropriate and effective for the task we are employing them for.

Our Processor Agreements outline:

- The processors data protection obligations
- Our expectations, rights and obligations
- The processing duration, aims and objectives
- The data subjects' rights and safeguarding measures
- The nature and purpose of the processing
- The type of personal data and categories of data subjects

We also ensure that we comply fully with Articles 28-29 of the GDPR and document in our agreements, that the processor:

- Processes the personal data only on our documented instructions
- Seeks our authorisation to transfer personal data to a third party (national/international organisation) unless required to do so by a law to which the processor is subject
- Shall inform us of any such legal requirement to transfer data before processing
- Ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality
- Takes all measures to security the personal data at all times
- Respects, supports and complies with our obligation to respond to requests for exercising the data subject's rights
- Assists the Trust in ensuring compliance with our obligations for data security, mitigating risks, breach notification and privacy impact assessments
- When requested, deletes or returns all personal data to the Trust after the end of the provision of services relating to processing, and deletes existing copies where possible
- Makes available to the Trust, all information necessary to demonstrate compliance with the obligations set out in the contract
- Allows and supports audits, monitoring, inspections and reporting as set out in the contract
- Informs the Trust immediately of any breaches, non-compliance or inability to carry out their duties as detailed in the contract

Please refer to our Data Protection Policy for more information.

7.7 Outsourcing Commencement

Upon completion of the agreement, the initial outsourcing commences on a trial period with regular monitoring checks. The process for outsourcing is as below: -

- If it is possible to outsource part of the service or to outsource in stages/sections, then this should be the default position for all service providers.

- Where the service provider has access to any internal systems, technical and physical access controls will be used and overseen by the Network Manager to prevent unauthorised access or data breaches.

- All existing in-house provisions and staff for the outsourced service, will be retained and made readily available throughout the initial implementation period to avoid delays or risks to the business or regulated activities.

- Reports are to be provided by the service provider to the Trust as per the agreed contract terms

- Monitoring checks will be carried out on a regular basis during the implementation period, to include:
    - Service/function quality
    - Regulatory compliance
    - Contractual compliance
    - Suitability
    - Efficiency

After the trial period of outsourcing, the terms of the service provision will be reviewed, to ensure that the outsourcing is viable and suitable on a long-term basis.

8. Monitoring & Audits

Monitoring of the quality, compliance and outcome of the outsourced service/process is carried out every 6/12 months to ensure that the service provider and outsourced function remain compliant with contractual and regulatory requirements and are both viable and suitable for business needs.

- Audit checklists are to be used when monitoring the performance and service provision of the outsourced service.

- Checklists are to be retained for 6 years after the working relationship has been terminated.

- Due diligence questionnaires are repeated on an annual basis with company and financial checks to be included.

To ensure the productivity, effectiveness and suitability of the outsourced service or process, the Trust ensures that the below key principles are, monitored and met, for the duration of the relationship:

- Compliance with the regulation, contractual and legal requirements is adhered to and maintained

- Continued measurements and assessment of the benefits and suitability against the projects initial criteria

- Ongoing risk assessments with any business and/or vendor changes and staff retention

- Training of new staff for both our business and the vendor

- Continual review and assessment of security and data protection standards and requirements

- Ongoing assessment that the vendor meets and achieves the SLA requirements and project criteria

- Audit and benchmarking measures and controls implemented, used and maintained

- Continued communication with the vendor throughout the business relationship

- Ensuring records and documentation are maintained and retained as per the SLA and legal requirements

- Dispute resolution and complaint monitoring

9. Responsibilities

The Trust has a corporate and regulatory obligation and responsibility to ensure that any service or business function that it outsources to a third-party service provider, is not subject to any operational risks or that there is not a loss of quality in the service provided.

The Chief Operating Officer has overall responsibility for handling all service provider contracts, SLA's, due diligence checks, audits and monitoring and for implementing and monitoring the Trust's procedures in relation to outsourcing. Management are responsible for designating suitable owners of business processes that are out sourced, overseeing the outsourcing activities and ensuring that this policy is followed. They also have full responsibility for mandating commercial or security controls to manage the risks arising from outsourcing.

Where the outsourced service or function relates to data protection or the personal information of an individual, the Data Protection Officer or lead is always involved in the planning, agreement and monitoring stages.

Appendix 1

INVICTUS
Education Trust

DATA PROCESSOR AGREEMENT *(TEMPLATE)*

This Data Processing agreement forms part of the [insert contract name] *("Principle Contract")* and is effective from _____ day of _____, 20___ *between* the undersigned parties:

Data Controller
Invictus Education Trust, Headquarters Kinver High School, Enville Road, Kinver DY7 6AA

And

Data Processor
[Processor Name], [Processor Trading Address]

1. Terms of Agreement

This agreement supplements the Principal Contract and makes legally binding provisions for compliance with the Data Protection Laws as set forth in this agreement. As per the requirements of relevant Data Protection Law, all processing of personal data by a Processor on behalf of a Controller, shall be, governed by a contract. The terms, obligations and rights set forth in this agreement relate directly to the processing activities and conditions laid out in Schedule 1.

The terms used in this agreement have the meanings as set out in the *'definitions'* part of the document, with any capitalised terms not otherwise defined, having have the meaning given to them in the Principal Contract.

2. Definitions

In this Agreement, unless the text specifically notes otherwise, the below words shall have the following meanings:

"Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law

"Consent" of the Data Subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her

"Data Protection Laws" means all applicable Data Protection Laws, including the General Data Protection Regulation (GDPR) (EU 2016/679), and, to the extent applicable, the data protection or privacy laws of any other country

"EEA" means the European Economic Area

"Effective Date" means that date that this agreement comes into force

"Personal data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

"GDPR" means the General Data Protection Regulation (GDPR) (EU) (2016/679)

"Principle Contract" means the main contract between the parties named in this agreement

"Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

"Processor" means a natural or legal person, public authority, agency or other body, which processes personal data on behalf of the Controller

"Recipient" means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities, which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law, shall not be regarded as recipients; the processing of those data by those public authorities shall comply with the applicable data protection rules according to the purposes of the processing

"Third-party" means a natural or legal person, public authority, agency or body other than the Data Subject, Controller, Processor and persons who, under the direct authority of the Controller or Processor, are authorised to process personal data

"Sub Processor" means any person or entity appointed by or on behalf of the Processor to process personal data on behalf of the Controller

"Supervisory authority" means an independent public authority, which is established by a Member State pursuant to Article 51 of the *"GDPR"*

3. Obligations and Rights of the Processor

The Processor shall comply with the relevant Data Protection Laws and must:

- only act on the written instructions of the controller
- ensure that people processing the data are subject to a duty of confidence
- ensure that any natural person acting under their authority who has access to personal data, does not process that data except on instructions from the Controller
- use its best endeavours to safeguard and protect all personal data from unauthorised or unlawful processing, including *(but not limited to)* accidental loss, destruction or damage and will ensure the security of processing through the demonstration and implementation of appropriate technical and organisational measures as specified in Schedule 1 of this agreement

- ensure that all processing meets the requirements of the GDPR and related Data Protection Laws and is in accordance with the Data Protection Principles

- ensure that where a sub-processor is used, they:

    - only engage a sub-processor with the prior consent of the data controller

    - inform the Controller of any intended changes concerning the addition or replacement of sub-processors

    - they implement a written contract containing the same data protection obligations as set out in this agreement, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Data Protection Laws

    - understand that where any sub-processor is used on their behalf, that any failure on the part of the sub-processor to comply with the Data Protection Laws or the relevant data processing agreement, the initial processor remains fully liable to the controller for the performance of the sub-processor's obligations

- assist the Data Controller in providing subject access and allowing Data Subjects to exercise their rights under the Data Protection Laws

- assist the Data Controller in meeting its data protection obligations in relation to:

    - the security of processing

    - data protection impact assessments

    - the investigation and notification of personal data breaches

- delete or return all personal data to the Controller as requested at the end of the contract

- make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in the relevant Data Protection Laws and allow for, and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller

- tell the Controller immediately if they have done something (*or are asked to do something*) infringing the GDPR or other Data Protection Law of the EU or a member state

- co-operate with Supervisory Authorities in accordance with GDPR Article 31

- notify the Controller of any personal data breaches in accordance with GDPR Article 33

- where applicable, employ a Data Protection Officer if required

- where applicable, appoint *(in writing)* a representative within the EU if required in accordance with GDPR Article 27

Nothing within this agreement relieves the Processor of their own direct responsibilities, obligations and liabilities under the General Data Protection Regulation *(GDPR)* or other Data Protection Laws.

The Processor is responsible for ensuring that each of its employees, agents, subcontractors or vendors are made aware of its obligations regarding the security and protection of the personal data and the terms set out in this agreement.

The Processor shall maintain induction and training programs that adequately reflect the Data Protection Law requirements and regulations, and ensure that all employees are afforded the time, resources and budget to undertake such training on a regular basis.

Any transfers of personal data to a third country or an international organisation shall only be carried out on documented instructions from the Controller unless required to do so by Union or Member State law. Where such a legal requirement exists, the processor shall inform the controller of that legal requirement before processing.

The processor shall maintain a record of all categories of processing activities carried out on behalf of the Controller, containing:

- the name and contact details of the Processor(s) and of each Controller on behalf of which the Processor is acting, and, where applicable, the Data Protection Officer
- the categories of processing carried out on behalf of each Controller
- transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, the documentation of suitable safeguards
- a general description of the technical and organisational security measures referred to in Article 32(1)
-

The Processor shall maintain records of processing activities in writing, including in electronic form and shall make the record available to the Supervisory Authority on request

When assessing the appropriate level of security and the subsequent technical and operational measures, the Processor shall consider the risks presented by any processing activities, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

4. Obligations and Rights of the Controller

The Controller is responsible for verifying the validity and suitability of the Processor before entering into a business relationship.

The Controller shall carry out adequate and appropriate on boarding and due diligence checks for all Processors, with a full assessment of the mandatory Data Protection Law requirements.

The Controller shall verify that the Processor has adequate and documented processes for data breaches, data retention and data transfers in place.

The Controller shall obtain evidence from the processor as to the:

- verification and reliability of the employees used by the Processor

- certificates, accreditations and policies as referred to in the due diligence processes
- technical and operational measures described in Schedule 1 of this agreement
- procedures in place for allowing Data Subjects to exercise their rights, including *(but not limited to*), subject access requests, erasure & rectification procedures and restriction of processing measures

Where the Controller has authorised the use of any sub-processor by the initial Processor, the Controller must verify that similar data protection agreements are in place between the initial Processor and sub-processor.

Where the Controller has authorised the use of any sub-processor by the initial Processor, the details of the sub-processor, must be added to Schedule 2 of this agreement.

5. Penalties & Termination

By signing this agreement, the Processor confirms that they understand the legal and enforcement actions that they may be subject to should they fail to uphold the agreement terms or breach the Data Protection Laws. If the Processor fails to meet their obligations, they may be subject to:

- investigative and corrective powers of Supervisory Authorities under Article 58 of the GDPR
- an administrative fine under Article 83 of the GDPR
- a penalty under Article 84 of the GDPR
- pay compensation under Article 82 of the GDPR

The Controller or Processor can terminate this agreement by [insert termination terms and notification periods].

6. General Information

[Insert any other clauses or terms specific to this Processor and the business relationship]

SCHEDULE 1

1. Processing Details

- The Controller named in this agreement has appointed the Processor with regard to specific processing activity requirements. These requirements relate to [insert subject matter].

- The duration of the processing is for/until [insert duration/end date/until further notice].

- The processing activities relate to [insert the nature] and are for the purpose of [insert purpose of the processing].

- The requirement for the named Processor to act on behalf of the Controller is with regard to the below type(s) of personal data and categories of Data Subjects:

    - [insert type(s) of personal data]
    - [insert categories of Data Subjects]

The Processor can demonstrate and provide sufficient guarantees as to the implementation of appropriate technical and organisational measures taken to ensure data security and protection:

- [insert technical measures]
- [insert organisational measures]

The obligations and rights of the Controller and Processor are set out in section (2) and (3) of this agreement.

SCHEDULE 2

Authorised Sub-Processor(s)

Sub-Processor 1

Name of Sub-Processor: _____

Address: _____

_____

_____

Telephone Number_____

Email Address_____

Type of Data Processed_____

_____

Authorised by Controller

Name_____ Date_____

Sub-Processor 2

Name of Sub-Processor: _____

Address: _____

_____

_____

Telephone Number_____

Email Address_____

Type of Data Processed_____

_____

Authorised by Controller

Name_____ Date_____

(Add other sub-processor and/or further schedules applicable/required by the business relationship for example contract clauses, binding corporate rules etc.)

IN WITNESS below of the parties or their duly authorised representatives have signed this agreement in accordance with all its clauses and on the day, month and year stated at the top of this agreement.

Signed on behalf of the Processor

Company Name:

Signed: _____

Print Name: _____

Position _____

Date: _____

Signed on behalf of the Controller

Company Name: Invictus Education Trust

Signed: _____

Print Name: _____

Position _____

Date: _____