INVICTUS

Education Trust

INVICTUS EDUCATION TRUST

GDPR MONITORING AND AUDIT POLICY & PROCEDURES

Approved by Board of Directors
2 July 2018

To be reviewed by Board of Directors
July 2021

Contents **Page**

Appendices

1. Policy Statement

An internal audit, as it applies to Invictus Education Trust is an independent and unbiased assessment and appraisal functions that reviews all operations, tasks, functions and business activities within our organisation. Audits are completed by varying staff members in accordance with the activity being reviewed.

This Monitoring & Internal Audit Policy & Procedures has been developed to assist the Trust and our staff in the assessment, monitoring, review and analysis of all business functions, procedures, systems and controls; with the aim of ensuring that all legal, contractual and regulatory standards and requirements are met, complied with and maintained.

It is our responsibility as a regulated company to carry out frequent audits on all procedures and to review the results and provide gap analysis information so that any short-comings or gaps can be assessed and corrected without negative consequences occurring, this reduced in the risk to our students, employees, customers, clients and associated third-parties.

The Trust has a responsibility to:

- establish, implement and maintain an audit plan to examine and evaluate the adequacy and effectiveness of the firm's systems, internal control mechanisms and arrangements

- monitor and evidence compliance with the relevant laws, regulations, contracts and codes of conduct as applicable to our organisation

- review processes and procedures on a frequent basis to ensure that they are still fit for purpose and adequately meet the requirements and purpose of the task they relate to

- keep abreast of laws and regulations that apply to the Company, to that procedures, controls and systems can be updated as soon as any changes or revisions occur

- provide feedback and appraisals to employees using monitoring and audit data

2. Purpose

The purpose of this policy is to provide the Trust’s statement of intent, objectives and methodical procedures, as they relate to compliance monitoring and internal audits, along with their associated procedures and documentation. The Trust carries out internal audits on all its employees, systems, processes and business activities in conjunction with the below objectives and in accordance with legal, contractual and regulatory guidance in all compliance areas, with the purpose of ensuring compliance, preventing breaches, assessing risks and protecting individuals and their personal data.

Our internal audit procedures are an assurance as to the effectiveness of the corporate governance, risk and compliance, business continuity management and internal controls. We aim to provide an independent and objective review of all business activities, operations, processing activities, financial systems, IT systems, and internal controls, through operational, financial and performance related audits. The procedures and related documents named herein, give the organisation and its employees, structure and guidance for carrying out internal audits.

3. Scope

This policy applies to all staff within the Trust *(meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with the Trust)*, and pertains to the processing of personal information. Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

The Data Protection Officer and school based Data Protection Compliance Officer are responsible for carrying out and/or overseeing all audits and ensures compliance with the below business areas. Where the process or activity relates to the processing of personal data or any data protection regulation. The Data Protection Officer can also appoint an audit team to assess and ensure compliance across the organisation.

- **Operational Audits**
- **Compliance Audits**
- **Financial Audits**
- **Anti-Money Laundering & Financial Crime Audits**
- **Information Security & Business Continuity Audits**
- **Data Protection & Processing Activity Audits**

4. Objectives

The Trust conducts internal audits with the objective of providing management information, to staff and third parties *(including clients, regulators, external auditors and suppliers),* and to ensure that efficient systems and processes are in place to achieve the overall business objectives.

The main objectives of our internal audits are to:

- Ensure compliance with regulatory, legal and contractual rules
- Ensure adherence to and compliance with any relevant codes of conduct or accreditation bodies as per education sector/industry requirements
- Prevent compliance breaches and exposure to risks
- Protection personal information and the individuals it belongs to
- Promote an anti-fraud, anti-money laundering & terrorist financing and anti-bribery corporate environment
- Provide assurance and give confidence to suppliers, customers and clients
- Assess the effectiveness and functionality of business activities
- Promote a culture of assessment, review and action to maintain growth and efficiency
- Keep systems and activities up-to-date in accordance with industry standards
- Provide a systematic and structured approach to assessment and review
- Maintain an audit history log for regulatory and investigative purposes
- Review and assess the effectiveness and adequacy of procedures, internal controls and systems
- Check for compliance breaches or risk based divergence from SOP's
- Ensure third party data is secure within the remit of the business activities
- Ensure the organisations assets and interests are adequately protected
- Ensure that risks are identified and mitigated against

4.1 Code of Ethics

The Data Protection Officer/Data Protection Compliance Officers or any Employee, who is allocated to complete an internal audit function, must adhere to the below code of ethics:

a) Competency – staff tasked with completing internal audits will have training and experience in this area and will continue an ongoing course of professional development in relation to audit procedures, industry standards and regulatory expectations. Staff will be knowledgeable and able to carry out audits in a consistent and capable manner and will apply these skills in the performance of the internal audit services.

b) Objectivity – staff who engage in any aspect on internal audit will remain objective, unbiased and be independent in both their approach and administering of the audit procedures. Information gathered for audit purposes will be done so in a professional and objective manner and will be used to adhere to the Trust's objectives, roles and responsibilities.

c) Confidentiality – internal audit staff will respect the information gathering during audits and will use the data solely for the purpose/s it is intended for. No information will be disclosed unless it is for specific audit purposes or is a legal, contractual or regulatory obligation

5. Compliance Monitoring & Internal Audit Procedures

The Trust will appoint a lead auditor, for the purposes of continuity and recourse but will also assign internal audit functions to supervisors, line managers, departmental managers and senior managers as the system or process necessitates. All staff engaging in audit procedures will hereafter, be referred to as *'Audit Staff'*.

The Audit Staff are responsible for utilising a systematic and disciplined approach to evaluating and assessing internal controls, systems and processes and to improve their effectiveness and efficiency as they relate to the business objectives.

Audit Staff are responsible for developing and maintaining a comprehensive audit program, which will include (but are not limited to):

- Audit Checklists
- Evaluation Plans
- Audit Policy
- Audit Procedures
- Audit Records
- Rolling Audit Assessments
- Due Diligence Third Party Checks

The audit program will ensure compliance with accounting standards, regulatory requirements, data protection laws, legal and contractual obligations, relevant accreditation and codes of conduct followed by the Trust and our own operating policies and procedures.

The Audit Staff are responsible for communicating all audit results and subsequent system/process changes with the relevant staff and to produce management information which will include, recommendations for alterations of any activities, practices or systems that do not meet the expected or required standards.

The Audit Staff are responsible for the development, evaluation, monitoring and review of the below audit areas.

5.1 Business Operational Audits

Such audits and monitoring are to assess educational/operational business activities and IT systems. The frequency of such audits is noted on the Compliance Monitoring Document, and are designed to ensure that the Trust is operating within our standard operating procedures for the education of students, business and employment law. This includes *(but is not limited to)* audits and assessments on as:

- Student Records – attendance, assessment, attainment, SEN, behaviour and welfare
- Staff Training, Development & Competence
- Complaints Procedures

- Records Management & Retention
- Internal Systems & Controls
- Risk Assessment Management
- HR Functions and Procedures
- Recruitment, Selection & Induction Processes
- Outsourcing & Due Diligence Procedures
- Management & Leadership Programs

These audits ensure that all processes and systems are at their most effective and efficient when assessed against the main business objectives and operating procedures.

5.2 Compliance Function Audits

These audits involve all business activities and systems that have an associated or direct impact on regulatory or legal compliance and are essential to the compliant functioning of the Trust. These areas include:

- Data Protection (GDPR)
- Freedom of Information Act
- Information & Physical Security
- Anti-Money Laundering & Financial Crime
- Anti-Bribery
- Health & Safety

These compliance audits serve the purpose of ensuring adherence to regulators rules, guidelines, laws and codes of conduct. They are audited on a frequent and rolling basis against the requirements of the relevant law or regulation.

5.3 Financial Audits

These audits review the accounting systems and processes and assess all financial transactions to ensure that all funds are being used, recorded and reported accurately and properly. Such audits must be carried out by staff who are trained and knowledgeable in the finance area, which will includes external auditors.

Financial audits determine if the internal controls governing the cash and assets associated with the organisation are effective, efficient and fit for purpose and that adequate process controls are in place to mitigate against financial crime.

5.3.1 Frequency of Audits

Audit frequency, is determined by the risk rating and regulatory implications of the business activity involved. Processes and systems are given an audit rating, and assigned a frequency dependant on the risk rating assigned. The audit rating takes into consideration how often the activity is performed, its regulatory impact, its risk rating and its priority as a business function or impact of non-compliance where the function relates to a legal or regulatory compliance area. This information is detailed on the Compliance Monitoring Document.

6.0 The Audit Program

6.1 Scope of Audit Program

To ensure complete coverage, the audit component of the compliance program includes testing of the firm’s compliance with specific regulatory and legal requirements as well as its own internal compliance policies and procedures. These seek to assess the adequacy of the compliance program itself, and provide a gap analysis report for senior management. Risk assessment procedures are detailed in the Risk Management Policy and are not included in this policy.

6.2 Methods and Audit Techniques

The methods of internal audits and checks include:

- **Physical Audit** – the auditor carries out the activity themselves to evaluate the process/system involved in the audit and to ensure compliance and functionality.

- **Monitored Audit** – the auditor assesses an employee carrying out a business activity to assess staff adherence to company procedures and regulatory compliance.

- **Email Reviews** – a sample of internal and external emails are reviewed to ensure compliance with business processes and compliance requirements.

- **Employee Interview*s*** – staff are involved in discussions about education/business activities and systems to ensure their knowledge and competence are at an acceptable level for the hired role.

- **Document Control** – existing procedures and policies are reviewed by the auditors to ensure they are fit for purpose, efficient and effective and that they adhere to regulatory requirements.

- **Risk Assessment** – mitigating strategies associated with each business activity are reviewed and followed to ensure that they mitigate against the associated risk and are fit for purpose.

6.2.1Development of the Audit Plan

The relevant designated person(s) is/are responsible for the development and integration of the Audit Plan, including those areas outlined in the Compliance Monitoring Programme Document and those unscheduled audits, required where errors and/or gaps have been identified.

The Trust creates an Audit Plan at the start of each year which documents the specific audits, staff, compliance areas and/or projects to be performed by the Internal Audit Team. The Audit Plan is then submitted to the Board of Directors for review and approval.

6.2.2 Communication

The Internal Audit Team will schedule a meeting with the department manager/s of the area, staff or process to be audited. They will relay the identified reason, scope and objectives of the audit, provides guidance on the estimated duration of the audit and ask for input prior to undertaking the review. Where any factors or issues have been raised, these are included in the audit notes.

All staff involved in the audit process are kept informed and are provided with guidance and information as applicable to the task being carried out. They are also kept informed on any findings and follow up reviews on a regular basis. In some instance, findings are addressed immediately.

6.3 Audit & Monitoring Process

Although the Trust recognises that every audit and/or project is unique, our audit process does follow similar steps for most areas, with an aim to minimise risks and increase efficiencies within the Trust.

The procedures for internal audits and compliance checks are as follows:

- Choose activity or system to be audited

- Determine a timeline. Since audits are often disruptive to daily functions, you should aim to allow the departments to maintain daily routines as much as possible, while still allotting time to complete the review thoroughly.

- Create a checklist of items that the auditor should observe when reviewing a file/task/account/employee.

- Use a ***Compliance Monitoring & Internal Audit Assessment Form (CMIA) (appendix 1)*** to log all methods and findings

- Obtain copy of the current activity procedure from document control

- Assess the process being performed against the steps on the procedural document and note any differences on the CMIA Form

- Determine a timeline. Since audits are often disruptive to daily functions, you should aim to allow the departments to maintain daily routines as much as possible, while still allotting time to complete the review thoroughly.

- List recommended actions if activity performed unsuccessfully

- Note audit log information on the CMIA Evaluation Plan

- Create Monitoring Impact report of audit results and communicate with relevant staff

All CMIA Forms are to be kept *(either electronically or as hard copies)* as an audit history log and used in conjunction with the CMIA Evaluation Plan.

Auditors must obtain all evidence necessary for the effective completion of the audit, for which the auditor's judgement based on experience, knowledge and intuition is to be used. A thorough knowledge of the concepts underlying audit evidence will help the auditor to improve the audit quality and efficiency of the process.

6.4 Auditor Expectations
It is common practice at the Trust, to utilise existing task procedures to carry out audits and to ensure that these procedures are suitable, up-to-date and compliant. However, any audit also necessitates utilising an auditor's opinions, observations, experience and recommendations as part of the audit process. To this end, all members of the Audit Team are obligated by professional standards to act objectively, exercise due professional care and collect sufficient and relevant information to provide a sound basis for audit observations and recommendations.

We ensure that where any staff member is expected to carry out audits, they hold sufficient skills, knowledge and experience to do so and that they meet all the regulatory requirements for performing an audit and monitoring role. We also provide all auditing staff with a thorough knowledge of the concepts underlying audit evidence and procedures, to better aid the auditor, improve the audit quality and maximise the efficiency of the process.

6.5 Audit Evidence
Whilst some audits are reliant solely on the following of existing procedures and ensuring that they are carried out in full and that those procedures are still fit for purpose and compliant, there is also a need to complete audits that require evidence and the collation of information. Where this is the case, the

evidence is expected to support the auditors in their role and to demonstrate sufficiency, competence and compliance.

Below are some of the evidence types used during our audit processes:

- **Physical Evidence** - obtained through observation, inquiry and existing documentation
- **Testimonial Evidence** – taken from interviews, statements and assessments from any person/s involved in the process being audited
- **Documentary Evidence** – consisting of any existing documents, reports, meeting minutes, contracts, procedures or records relevant to the audit process and/or the task/person being reviewed
- **Analytical Evidence** – gathered and documented through the analysis of any information collected by the auditor during the audit
- **Procedure Evidence** – utilising existing task procedures to complete a walk-through of the task completion and auditing standards against those procedures

7. Reference Documents

Documents and procedures associated with this policy are as below:

- Compliance Monitoring Document
- Data Protection Policy & Procedures
- Data Protection Impact Assessment Procedures
- Risk Management Policy and Procedures
- Data Breach Procedures
- IT Policies and Procedures

The Trust's roles and responsibilities as they relate to compliance monitoring and internal audits are to:

- review and assess the effectiveness and adequacy of procedures, internal controls and systems
- check for compliance breaches or risk based divergence from SOP's
- ensure that the desired level of quality assurance is maintained
- ensure that staff are offering the accurate, appropriate and compliant advice, products and services
- ensure that student/parent/employee/third party risks are identified and mitigated against

The Board of Trustees has overall responsibility for the monitoring and audit process, associated reviews and management information and reporting, however all managers must take accountability for their own staff and department areas and follow a consistent program of staff monitoring and training

Appendix 1

INVICTUS
Education Trust

Compliance Monitoring & Internal Audit Assessment Form (CMIA)

Auditors Name:	**Date:**
Location of Audit:	
Activity/process being audited:	
Variations from Procedural Document or Regulations:	

Cause/s for Variation: *(if applicable)*

Actions/Recommendations:

Procedure Document Used	**Auditing Method**	**Next Audit Date**

Auditor’s Signature:

Data added to CMIA Plan: