Burnley College
Counter Fraud Statement and Action Plan
2025-26

Introduction

As with other organisations the College is at risk of losses through fraud, bribery and corruption. The College recognises that as well as causing financial loss such activities are also detrimental to the provision of services and damaging to the reputation of the College. To safeguard itself the College is committed to making sure that the opportunity for fraud, bribery and corruption is reduced to the lowest possible risk within existing resources.

This statement outlines the College's commitment and approach to tackling fraud, bribery and corruption and applies to all those who work for, or interact with the College including employees, Governors, contractors, suppliers and students. Fraud against the College is not acceptable in any form and the College will seek full redress through criminal and/or civil courts to counter any internal or external fraudulent activities perpetrated against it.

Aims & objectives

The general aims and objectives of this statement are to:

1. create and promote a robust "anti-fraud" culture across the organisation, highlighting the College's zero tolerance of fraud, bribery and corruption, which is also acknowledged by others outside the College.
2. encourage individuals to promptly report suspicions of fraudulent or corrupt behaviour and provide them with effective means for doing so.
3. protect the College's valuable resources and minimise the likelihood and extent of losses through fraud and corruption.
4. enable the College to apply appropriate sanctions and recover all losses.
5. work with partners and other investigative bodies to strengthen and continuously improve the College's resilience to fraud and corruption.

This statement contributes towards the achievement of the College's Strategic Goals, in particular Goal 8, "To achieve the College budget while demonstrating value for money, and environmental sustainability", by increasing the College's resilience against fraud, bribery and corruption, thereby minimising the extent of losses and maximising the financial resources available to achieve positive outcomes for the College community.

Responsibility

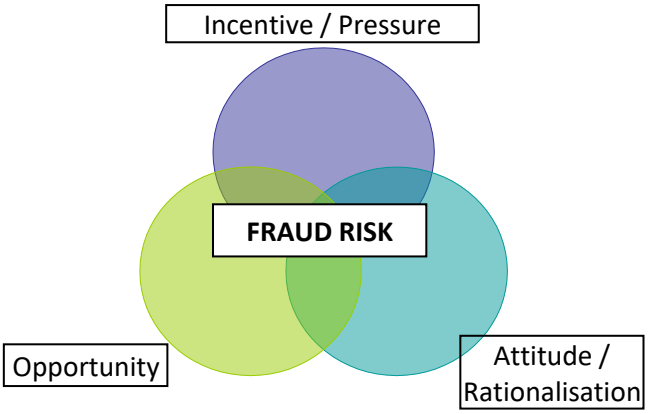
The Principal has overall responsibility for the operation of the College in respect of counter fraud culture and activities, with the Director of Finance and Resources taking the Strategic Lead for the maintenance and operation of the overarching Counter Fraud Statement and actions to ensure that it continues to remain compliant and meet the requirements of the College.

All Managers are responsible for fraud risk management in their particular area with support from the Senior Management Team. Management should embed strong counter fraud controls and systems; support counter fraud and corruption activities and training; and ensure other governance papers, strategies and policies include fraud and corruption risks wherever relevant.

The Audit Committee monitors the effectiveness of the control environment, including arrangements for ensuring value for money and for managing the College's exposure to the risk of fraud and corruption.

Heightened threat of fraud

There are three conditions that are commonly found when fraud occurs:



The perpetrators experience some incentive or pressure to engage in misconduct. There must be an opportunity to commit fraud and the perpetrators are often able to rationalise or justify their actions.

The current economic climate in the United Kingdom and the Government policy of significantly reduced public spending have the potential to increase the risk of fraud. During these periods of uncertainty, whether at a national or local level, it is essential that the College continues to maintain strong defences against fraud and irregularity. Enhanced focus on fraud awareness and deterrence will be crucial, ensuring all resources are effectively managed to mitigate the risk of fraud. This will involve working closely with partners, contractors and suppliers to overcome any barriers to effective fraud fighting and making the best use of available information and intelligence.

Loss and harm caused by fraud

Losses from fraud are evident in a range of public and private sector services such as education, healthcare, government, insurance and agriculture. The annual financial cost of fraud in the UK is estimated at £219 billion (Source: Annual Fraud Indicator 2023: Identifying the cost of fraud to the UK economy), which is broken down as follows:

Private Sector	£ 157.8 billion
Public Sector	£ 50.2 billion
Individuals	£ 8.3 billion

These figures represent a significant increase over 4 years and clearly show the significant risk that fraud poses to all organisation, including the College and the potential impact it could have the College's finances.

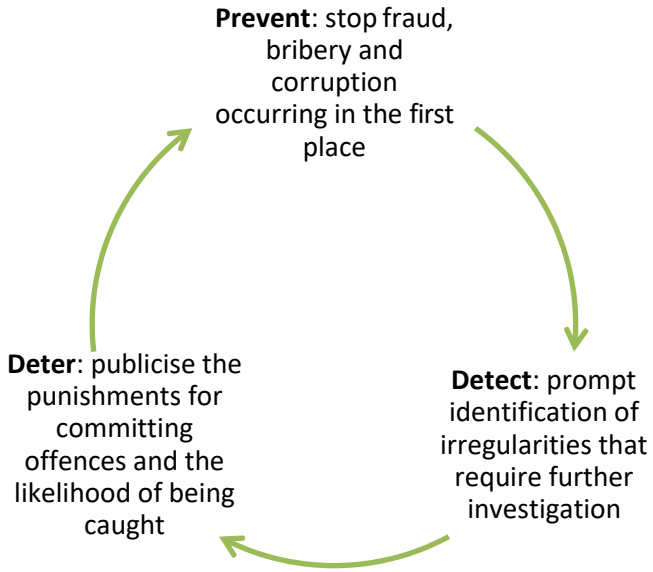
Risk assessment and action plan

A counter fraud statement working group was established, made up of managers from the key areas of the College where fraud is most likely to occur, to develop a Counter Fraud Risk Assessment (see Annex 1).

This risk assessment identifies the areas that fraud risk is highest within the College, the risks that the organisation faces, the potential impact if that risk materialised, and the controls that are already in place to combat the risk. Any further action needed to further reduce the risk has also been recorded against each risk, using the approach detailed in the section below. Please see Annex 1 for the detailed risk assessment.

Approach to countering fraud

The College's approach for meeting the aims and objectives of the statement and addressing fraud, bribery and corruption focuses on three core elements:



Prevent

Everyone who works for, or with, the College has a responsibility for ensuring public funds and resources are being used appropriately. The College promotes a zero-tolerance culture where fraud, bribery and corruption are recognised as unacceptable behaviour.

Prevention of fraud, bribery and corruption against the College will focus on:

- the identification and routine evaluation of fraud risks to understand specific exposures to risk, changing patterns in fraud and corruption threats and the potential consequences to the College and its users.
- maintaining a counter-fraud culture to increase resilience to fraud.
- preventing fraud through the implementation of appropriate and robust internal controls and security measures.
- developing networks, protocols and arrangements to facilitate joint working or partnerships to manage the College's fraud risks.

Detect

Despite the best efforts to prevent fraud occurring in the first place, it is difficult to eradicate it from the system entirely. Therefore, measures need to be in place to ensure inappropriate activity is detected and reported for further investigation. Detection and investigation is a key priority of this statement which will be bolstered by:

- ensuring protocols are in place to facilitate data and intelligence sharing and analysis, using techniques such as data matching and data analytics, to validate data and detect control failings to support counter fraud activity.
- maintaining and enhancing effective whistleblowing arrangements.
- effectively investigating fraud referrals.
- utilising an appropriate mix of experienced and skilled staff and consultants including access to counter fraud specialists with professional accreditation.

Deter

The College recognises the importance of deterring individuals from committing fraud, bribery and corruption by:

- communicating the College's anti-fraud and corruption stance and the actions it takes against fraudsters.
- applying sanctions, including internal disciplinary, regulatory and criminal.
- seeking redress, including the recovery of assets and money where possible.

Review and assessment

This Counter Fraud Statement, including the Risk Assessment will be reviewed on an annual basis and presented to the College's Audit Committee along with a report summarising updates to fraud risk, actions and improvements the College has made.

Annex 1 - Counter Fraud Risk Assessment and Action Plan

Area (eg. IT, Finance, HR)	Risk / Threat	Description of Potential Impact	Controls in place	Impact Score (out of 5)	Likelihood Score (out of 5)	Risk Score (Impact x Likelihood) and Rating	Actions required (Prevent, Detect, Deter)
IT (Network Services Manager)	Impersonation of staff member through hijacking of account	Fraud perpetrated in name of College. Reputational impact	Firewall controls, email spam filtering, impersonation protection, routine checks on unusual activity	2	2	4 Minor	Prevent - Communicate importance of safe use of systems, secure use of passwords
IT (Network Services Manager)	Phishing and email scams	Access to personal information/College systems that could be used to commit fraud	Firewall controls, email spam filtering, impersonation protection, routine checks on unusual activity	2	4	8 Medium	Detect - Review of email spam activity. Prevent - identification of targeted users for additional training, training and test emails for staff
IT (Network Services Manager)	Cryptolocker/ransomware hack	Inability to use one or more College systems, downtime while data is restored	Firewall controls, strict AV policies, backups of offsite data	5	2	10 High	Prevent - Increase use of cloud backups with no link to vulnerable systems, multi-factor authentication Detect – anti-virus and firewall solutions to be kept up to date
IT (Network Services Manager)	Abuse of network administrator access by IT staff to commit fraud	Criminal prosecution of staff, failure of audit, reputational impact	Separation of responsibilities, local accounts used where possible, monitoring of admin accounts, culture of ethical behaviour	5	1	5 Medium	Prevent - Continuous review of best practice and embedding of culture of openness and ethical use of admin access.
IT (Network Services Manager)	Abuse of procurement process	Criminal prosecution of staff, failure of audit, reputational impact	Policies and Procedures, use of procurement frameworks checks and balances	3	1	3 Minor	Prevent - Ensure policies and procedures are followed. Culture that reinforces integrity in dealing with suppliers

Area (eg. IT, Finance, HR)	Risk / Threat	Description of Potential Impact	Controls in place	Impact Score (out of 5)	Likelihood Score (out of 5)	Risk Score (Impact x Likelihood) and Rating	Actions required (Prevent, Detect, Deter)
			through multiple teams involved in procurement.				
MIS (Funding Compliance Manager)	Creation of "fake" enrolments by staff member	Criminal prosecution, failed audit, reduction/removal of contracts by funding agencies	Policies and procedures to confirm student existence and eligibility, internal and external audit.	5	1	5 Medium	Detect - Continuous review of College data. Prevent - culture of integrity embedded via management team
MIS (Funding Compliance Manager)	Falsification of learner eligibility/validity by learner - claiming support/funding without entitlement	Failure of audit, loss of funding for entitled learners	Policies and procedures to confirm student entitlement, internal and external audit	2	2	6 Medium	Prevent - Training for all staff involved in data entry. Validation checks.
Tills (Finance Manager)	Cash stolen from tills by staff	Loss of cash through theft by staff	Reconciliation of cash to till reports. CCTV in canteens.	2	2	4 Minor	Detect – additional check between stock levels and till receipts. Prevent – reduced use of cash on site through card and digital technologies
Commercial (Finance Manager)	Cash payments for courses being stolen	Loss of cash through theft by staff	Reconciliation of cash to till reports and fee receipts to course reports	2	2	4 Minor	Deter – communication of penalties for committing fraud Prevent – training on correct processes and culture
Reprographics (Head of Central Services)	Cash payments for printing	Loss of cash through theft by staff	Reconciliation of cash to till reports	2	2	4 Minor	Deter – communication of penalties for committing fraud Prevent – training on correct processes and culture

Area (eg. IT, Finance, HR)	Risk / Threat	Description of Potential Impact	Controls in place	Impact Score (out of 5)	Likelihood Score (out of 5)	Risk Score (Impact x Likelihood) and Rating	Actions required (Prevent, Detect, Deter)
Finance (Finance Manager)	Change of supplier bank details	Payments could be made to fraudster rather than a company.	Any email or letter asking for a change of bank details is followed up with a phone call to the company using a number known to ourselves already. Notes of this check must be added to the system. Finance system alerts Finance Manager of any bank detail changes. Any changes are reviewed prior to payment by first approver to make sure the checks have been completed. Confirmation that these steps have happened is sent to second approver prior to payment sign off.	4	1	4 Minor	Detect – additional spot checks on bank details by separate person Prevent – training on correct processes to be followed. Deter – communication of penalties for committing fraud.

Area (eg. IT, Finance, HR)	Risk / Threat	Description of Potential Impact	Controls in place	Impact Score (out of 5)	Likelihood Score (out of 5)	Risk Score (Impact x Likelihood) and Rating	Actions required (Prevent, Detect, Deter)
Finance (Finance Manager)	Fraudulent emails from a Manager, asking for payment to be made.	A payment request could mean making payment that hasn't been authorised.	Any email is followed up by communicating with the Manager by phone or other means before payments are made. Password check process in place with Principal.	4	1	4 Minor	Prevent – refresher training for staff to ensure correct processes followed. Detect – liaison with IT if false email suspected.
Finance (Finance Manager)	Invoices received for goods or services not supplied.	A payment could be made that is not due.	Invoices are checked and matched to a Goods Receipt Note (GRN) or authorised by a Manager.	3	1	3 Minor	Deter – reminder to suppliers of correct College processes and timings for invoices and payments. Prevent – training for staff on correct processes.
Finance (Finance Manager)	The same member of staff could enter a GRN on the system and pay the invoice against it.	Fraudulent invoices could be paid.	Segregation of duties and electronic authorisation methods set on Ebis.	3	1	3 Minor	Deter – communication of penalties for committing fraud. Detect – check of invoices at payment stage by separate person.
Finance (Finance Manager)	No sales and void transactions on the till	Money could be taken for a transaction and then the transaction voided and cash retained by fraudster	Void access only given to manager. Voids recorded on the till system and questioned by finance cashier	3	2	6 Medium	Deter – communication of penalties for committing fraud. Prevent – training for staff on correct processes.

Area (eg. IT, Finance, HR)	Risk / Threat	Description of Potential Impact	Controls in place	Impact Score (out of 5)	Likelihood Score (out of 5)	Risk Score (Impact x Likelihood) and Rating	Actions required (Prevent, Detect, Deter)
Finance (Finance Manager)	Fake supplier set up	Invoices could be raised and paid to fraudster	Finance system alerts Finance Manager to any new suppliers. Payment runs are checked by Finance Manager who interrogates new suppliers.	3	2	6 Medium	Deter – communication of penalties for committing fraud. Prevent – training for staff on correct processes.
Finance (Finance Manager)	Purchases made for personal use	Purchasing Officer could purchase items on college credit card for personal use	Purchasing paperwork must be authorised by a manager, Credit card statement is reconciled and file is signed off by finance manager.	3	2	6 Medium	Deter – communication of penalties for committing fraud. Prevent – training for staff on correct processes.
Finance (Finance Manager)	Petty cash irregularities	Cash could be stolen by member of staff or a fake petty cash slip provided	Petty cash can only be accessed by finance team. It is reconciled twice a week to ensure no discrepancies.	2	1	2 Negligible	Deter – communication of penalties for committing fraud. Prevent – training for staff on correct processes.
Finance (Finance Manager)	Access to college safe	Limited amount of cash is stored within which could be taken.	There are only three safe keys for the college safe which are held by key finance team members	2	1	2 Negligible	Deter – communication of penalties for committing fraud. Prevent – training for staff on correct processes. Detect – regular checks and reconciliations of cash held in safe.

Area (eg. IT, Finance, HR)	Risk / Threat	Description of Potential Impact	Controls in place	Impact Score (out of 5)	Likelihood Score (out of 5)	Risk Score (Impact x Likelihood) and Rating	Actions required (Prevent, Detect, Deter)
HR/ Payroll (HR Manager)	False additions to salary	Anyone with full access to the HR system, increasing theirs/others' salary	Full access to the system is rare and only held by some members of the IT and HR teams. Payroll auditing reports and checking procedures highlight changes made each month and any increases to salary	4	1	4 Minor	Prevent - Pre-employment (including DBS) checks Prevent - Fraud prevention training at induction Detect - Allegations of any such misconduct would be investigated and if found to have happened, disciplinary sanctions issued. Deter - Where any such misconduct resulted in dismissal, sensitively communicate the serious consequences throughout the organisation
HR/ Payroll (HR Manager)	Ghost employee receiving a salary	Anyone with full access to the HR system, adding a non-existent employee to whom a salary is paid	Full access to the system is rare and only held by some members of the IT and HR teams. Payroll auditing reports and checking procedures allow for effective comparison of headcount (including the starters and leavers in the relevant	5	1	5 Medium	Prevent - Fraud screening at recruitment stage – particularly for certain teams and for all budget holders – including DBS and reference checks Prevent - Fraud prevention training at induction Detect - Allegations of any such misconduct would be investigated and if found to

Area (eg. IT, Finance, HR)	Risk / Threat	Description of Potential Impact	Controls in place	Impact Score (out of 5)	Likelihood Score (out of 5)	Risk Score (Impact x Likelihood) and Rating	Actions required (Prevent, Detect, Deter)
			month) and payments made, including where employees have salary paid into more than one account and where more than one employee shares the same bank account				have happened, disciplinary sanctions issued. Deter - Where any such misconduct resulted in dismissal, sensitively communicate the serious consequences throughout the organisation
HR/ Payroll (HR Manager)	Changes to employee's sensitive information	Anyone with full access to the HR system, changing the details of an existing employee for any reason, or obtaining someone else's details with the intention of committing identify fraud	Full access to the system is rare and only held by some members of the IT and HR teams. To change bank details, employees must submit a signed paper document, in person.	5	1	5 Medium	Prevent - Fraud screening at recruitment stage – particularly for certain teams and for all budget holders – including DBS and reference checks Prevent - Fraud prevention training at induction Detect - Allegations of any such misconduct would be investigated and if found to have happened, disciplinary sanctions issued. Deter - Where any such misconduct resulted in dismissal, sensitively communicate the serious consequences throughout the organisation

Area (eg. IT, Finance, HR)	Risk / Threat	Description of Potential Impact	Controls in place	Impact Score (out of 5)	Likelihood Score (out of 5)	Risk Score (Impact x Likelihood) and Rating	Actions required (Prevent, Detect, Deter)
HR/ Payroll (HR Manager)	Fraudulent claims for hours worked	Staff claiming for more hours than they worked, or claiming the rate of a higher role when not working in that position	Hourly paid teaching staff are paid via their registers so they are only paid once a register has been marked, which accurately reflects a viable class. For other staff who claim their hours, managers understand the importance of checking all claims, to ensure the hours claimed accurately reflect the hours worked and they can cross check claims against timetables. The PTHP spend is closely monitored and reviewed by SMT which helps to ensure managers check they are correct before payment	3	3	9 Medium	Prevent/Detect - Managers must check and authorise all pay claims, as well as reviewing registers regularly to ensure any updates are applied. Prevent - New managers must be trained on the use of College systems Detect - Allegations of any such misconduct would be investigated and if found to have happened, disciplinary sanctions issued. Deter - Where any such misconduct resulted in dismissal, sensitively communicate the serious consequences throughout the organisation

Area (eg. IT, Finance, HR)	Risk / Threat	Description of Potential Impact	Controls in place	Impact Score (out of 5)	Likelihood Score (out of 5)	Risk Score (Impact x Likelihood) and Rating	Actions required (Prevent, Detect, Deter)
HR/ Payroll (HR Manager)	Fraudulent claims for PT sessions at Fitness Evolution (FEVO)	Staff claiming they have carried out PTs/more PTs than they actually have	Staff understand their obligations to provide receipts and to ensure that PTs go through the till in order to be paid. The system by which PTs are paid is reviewed regularly by SMT, the FEVO manager and HR. Receipts from PT sessions are compared to the till receipts from FEVO by the manager, HR and SMT	3	2	6 Medium	Prevent/Detect - FEVO managers must check and authorise all pay claims, as well as reviewing registers regularly to ensure any updates are applied. Prevent - New FEVO managers/coordinators must be trained on the use of College systems Prevent - New PT staff must be trained in the required processes, including the potential for fraud and the zero-tolerance approach to any fraud Detect - Allegations of any such misconduct would be investigated and if found to have happened, disciplinary sanctions issued. Deter - Where any such misconduct resulted in dismissal, sensitively communicate the serious consequences throughout the organisation

Area (eg. IT, Finance, HR)	Risk / Threat	Description of Potential Impact	Controls in place	Impact Score (out of 5)	Likelihood Score (out of 5)	Risk Score (Impact x Likelihood) and Rating	Actions required (Prevent, Detect, Deter)
HR/ Payroll/ Finance (Finance Manager)	Falsely procuring goods for personal use through College budgets	Budget holders signing purchase requests off for items intended for personal use	The only budget holders are managers and any spend is visible by the Finance team and SMT. Senior managers' check items of significant amount and all spend is monitored closely, with monthly budget/spend information produced and questions asked of purchases made. Managers do know they should inform their SMT member should they require a costly item and justify the purchase	4	2	8 Medium	Prevent - Fraud screening at recruitment stage – particularly for certain teams and for all budget holders – including DBS and reference checks Prevent - Fraud prevention training at induction Detect - Allegations of any such misconduct would be investigated and if found to have happened, disciplinary sanctions issued. Deter - Where any such misconduct resulted in dismissal, sensitively communicate the serious consequences throughout the organisation

Area (eg. IT, Finance, HR)	Risk / Threat	Description of Potential Impact	Controls in place	Impact Score (out of 5)	Likelihood Score (out of 5)	Risk Score (Impact x Likelihood) and Rating	Actions required (Prevent, Detect, Deter)
HR/ Payroll/ Finance (Finance Manager)	Fraudulent expense claims including mileage and food and falsely naming trips away/visits as business meetings	Employees claim more mileage than travelled and/or claim expenses accumulated on personal trips, names as business trips	Senior managers review and question mileage claims and compare with diaries to verify trips	4	2	8 Medium	Prevent - Fraud screening at recruitment stage – particularly for certain teams and for all budget holders – including DBS and reference checks Prevent - Fraud prevention training at induction Instructions on the circumstances when expenses can be claimed back delivered at induction, including mileage. Detect - Allegations of any such misconduct would be investigated and if found to have happened, disciplinary sanctions issued. Deter - Where any such misconduct resulted in dismissal, sensitively communicate the serious consequences throughout the organisation
Academic (Deputy Principal)	Fraudulent claim for qualification certification from a member of staff due to staff error, staff	A member of staff falsely claims certification for a student or provides	Divisional managers check and sign off qualification claims before submission to	3	2	6 Medium	Prevent – Checking of evidence and data entry at multiple points in the process.

Area (eg. IT, Finance, HR)	Risk / Threat	Description of Potential Impact	Controls in place	Impact Score (out of 5)	Likelihood Score (out of 5)	Risk Score (Impact x Likelihood) and Rating	Actions required (Prevent, Detect, Deter)
	fraud or student fraud. This could lead to reputational damage as well as financial loss and withdrawal of awarding body approval.	false grades for the claim of the qualification.	the College exams team who conduct further checks and sample audits of evidence. Internal and external verification process of grades and claims by independent staff and externals.				Prevent – automation of grade calculation based on assignment and exams marks. Detect – multiple checks throughout the process. Deter – clear implications for any issues identified, including dismissal.

SCORING RISKS

ASSESSMENT OF RISK IMPACT – these descriptions should be used as a guide only with each risk considered on a case by case basis.

Rating	1 Minimal	2 Minor	3 Moderate	4 Major	5 Catastrophic
Financial	Less than £5,000	£5,000 or more, but less than £25,000	£25,000 or more, but less than £100,000	£100,000 or more, but less than £1,000,000	More than £1,000,000.
Health & Safety	Incident but no injury	Minor medical treatment only	Lost time / moderate injury RIDDOR	Disability or HSE enforcement	Fatality or prosecution by the HSE
Customer Service	Minor complaints received	Widespread complaints	Complaints and investigation to the regulator	Repeated minor intervention by regulator	Formal action under by the regulator
Reputation	Minor adverse local media coverage	Adverse local media coverage	Adverse regional or national media coverage	Sustained adverse media coverage at various levels	Formal action by the regulator
Legislative and Regulatory	Minor breaches by employees resulting in minor adverse publicity	Infringements of regulations / legislation resulting in minor fines or adverse publicity	Legal action taken against the College	Significant Litigation/Fines or Prison sentences for Directors of Officers.	Forced closure of the College
Organisational	Absorbed without additional management activity	Absorbed with minimal management activity	Significant event which requires specific management	Critical event which can be endured with targeted input	Disaster which can cause collapse of the business
Business Continuity	Minor disruption to services at one site	Minor disruption to services at multiple sites	Moderate disruption at multiple sites, short term closure of a site	Temporary closure of multiple sites leading to severe disruption of services	Complete closure of a main site
Performance	Minor reduction in performance in one area.	Sustained reduction in performance in one area or reduction in performance across several areas.	Sustained reduction in performance in more than one area.	Sustained non-performance resulting in formal action by the regulator	Regulator steps in and takes control of or closes the College.

ASSESSMENT OF PROBABILITY/LIKELIHOOD

RATING	DESCRIPTOR	DESCRIPTION	PROBABILITY	INDICATIVE FREQUENCY
5	Almost Certain	Is expected to occur	96 – 100%	At least one event per year
4	Likely	It will probably occur	76 – 95 %	One event per year on average
3	Possible	May occur	21 – 75%	One event per 2 – 10 years
2	Unlikely	Not likely to occur	6 – 20%	One event per 11 – 50 years
1	Rare	Most unlikely to occur	0 – 5%	One event per 51 – 100 years

RISK RATING (LIKELIHOOD X IMPACT)

	IMPACT				
LIKELIHOOD	Minimal (1)	Minor (2)	Moderate (3)	Major (4)	Catastrophic (5)
Almost Certain (5)	*Medium*	*High*	*High*	*Extreme*	*Extreme*
Likely (4)	*Minor*	*Medium*	*High*	*High*	*Extreme*
Possible (3)	*Minor*	*Medium*	*Medium*	*High*	*High*
Unlikely (2)	*Negligible*	*Minor*	*Medium*	*Medium*	*High*
Rare (1)	*Negligible*	*Negligible*	*Minor*	*Minor*	*Medium*

Risk Ratings

	>16		10-16		5-9		3-4		<3
	Extreme		High		Medium		Minor		Negligible