

## Risk Assessment



Area: Regulation & Compliance Date: 12/10/2021 Assessment number: RC/DP/R 1

Staff responsible: Principal & CM Review Date: 30/06/2022

Task: **GDPR COMPLIANCE**

Risk Number	Risk Description	Effects/ Impact on	Existing controls	Risk Rating			Further action required/ action plan	By Whom	Date	Cross reference categories	Risk with Mitigation	Update
				Impact (I)	Likelihood (L)	Rating						
1	Failure to secure electronic records including BB & 'O' Drive	Patients/students/staff. College reputation and business viability locally & nationally	GDPR Governor & Officers; Pw protection practices; Server with access securities; Policies & staff awareness/ training Removal & update of data policy & practice. Issuing of College email addresses	Medium (3)	Possible (2)	Medium (6)	Policy and protocol in handbook	SMT & CM	January 2022		Medium	
2	Failure to secure onsite paper records/files	Patients/students/staff. College reputation and business viability locally & nationally	Data in secure locked files/offices. Policy for data destruction Confidential shredding annually. Securities applied to file access	Medium (3)	Possible (2)	Medium (6)					Low	
3	Failure deal correctly with archived /out of date data	Patients/students/staff. College reputation and business viability locally & nationally	College policy for file retention & destruction Equipment to deal with smallscale daily shredding of confidential material Certified shredding company used annually.	Medium (3)	Possible (2)	Medium (6)	None				Low	
4	Visual displays	Patients/students/staff. College reputation and business viability locally & nationally	Policy & Practice of not displaying sensitive information & data in 'public' places/notice boards.	Medium (3)	Possible (2)	Medium (6)				GDPR RA 2	Low	
5	Failure to communicate data institution's policy & practices	Patients/students/staff. College reputation and business viability locally & nationally	Policies displayed on Intranet, in clinic or on general noticeboards.	Medium (3)	Possible (2)	Medium (6)	Populate new staff area on blackboard with appropriate policies.		31.1.22		Medium	

**Risk Assessment**

Low
Medium
High

Area	Regulation & Compliance	Date	12/10/2021	Assessment number	RC/F/R2
------	-------------------------	------	------------	-------------------	---------

Staff responsible	Bursar	Review Date	30/06/2022
-------------------	--------	-------------	------------

Task	<b>FINANCE FRAUD</b>
------	----------------------

Risk Number	Risk Description	Effects/ Impact on	Existing controls	Risk Rating			Further action required/ action plan	By Whom	Date	Cross reference categories	Risk with Mitigation	Update
				Impact (I)	Likelihood (L)	Rating						
1	Electronic/online banking fraud	Budget inaccuracies , possible financial losses to the College. Professionalism queries - contract competency expectations breached	Online banking access restricted to Gov finance, bursar & Pr. Individual access /PWS. Finance Reports to subfinance & BoG. Annual audit, 3yr external audit check.	High (4)	Possible (2)	High (8)	Written Finance (online banking) Protocol	BoG (F) & Bursar	April 2022		Medium	
2	Telephone banking fraud	Budget inaccuracies , possible financial losses to the College. Professionalism queries - contract competency expectations breached	Telephone banking access restricted to Gov finance, bursar & Pr. Individual access require pws. Finance reports to sub-finance & BoG. Annual audit, 3yr external audit check.	High (4)	Possible (2)	High (8)	Written Finance (telephone banking) Protocol	BoG (F) & Bursar	April 2022		Medium	
3	Student fee collection (SFE, ELCAS, self funding) fraud	Budget inaccuracies , possible financial losses to the College. Professionalism queries -contract competency expectations breached	SFE: Franchise arrangement - University SFE payment checks & re-imbursment initiation: Validation arrangement - College payment checks & re-imbursment initiation. ELCAS/self funding - College payment checks & re-imbursment initiation. Student Contract, Student Protection Plan , Credit Control & Refund & Compensation Policies	High (4)	Possible (2)	High (8)	Timeframe and documentation required made clear to students, (produce flow diagram)	Bursar	January 2022		Low	
4	Fraudulent use of resources e.g phone/copiers etc	Budget inaccuracies , possible financial losses to the College. Professionalism queries - contract competency expectations breached	Monthly checks e.g. on Phone usage against bills & photocopy use. Stock monitoring of resources by CL Leads	Medium (3)	Possible (2)	Medium (6)	None				Low	
5	Fraudulent claims -work/hours	Budget inaccuracies , possible financial losses to the College. Professionalism queriescontract competency expectations breached	Staff pay claim submission, checks initiated by bursar only	High (4)	Possible (2)	High (8)					Low	
6	Fraudulent (Patient Fees collection, recording & banking)	Budget inaccuracies , possible financial losses to the College- contract competency expectations breached	Receptionist/lead clinician end of session till checks, Monthly Bursar checks, Clinical leads.	High (4)	Possible (2)	High (8)	Written Protocol for collecting recording & banking	Bursar	January 2022		Medium	

**Risk Assessment**

Low
Medium
High

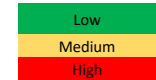
Area	Regulation & Compliance	Date	12/10/2021	Assessment number	RC/IT/R3
------	-------------------------	------	------------	-------------------	----------

Staff responsible	Principal	Review Date	30/06/2022
-------------------	-----------	-------------	------------

Task	<b>IT SECURITY</b>
------	--------------------

Risk Number	Risk Description	Effects/ Impact on	Existing controls	Risk Rating			Further action required/ action plan	By Whom	Date	Cross reference categories	Risk with Mitigation	Update
				Impact (I)	Likelihood (L)	Rating						
1	Hacking of Website	People: Staff, students (potential, current & alumni), patients and the public. College business & partners	QH Service Level Agreement, website maintenance & checks (F1), Firewalls,	High (4)	Possible (2)	High (8)					Low	
2	Security breach of confidential areas on College intranet / access to unauthorised data	People: Students (potential, current & alumni), patients and the public. College business & collaborative partners	O Drive set up with Access rights, SLA with QH, monitoring by SMT authorisation access & changes via Pr only, PW protected transfer of data.	High (4)	Possible (2)	High (8)	None				Low	
3	Virus /phishing attack	People: Staff, students (potential, current & alumni), patients. College business & collaborative partners	QH Service Level Agreement, Firewalls, regular software updates, website maintenance & checks (F1),	High (4)	Possible (2)	High (8)	None				Low	
4	loss of portable hardware e.g. laptop/ Ipad, or PC	People: Staff, students (potential, current & alumni), patients. College business & collaborative partners	Password protection. Access securities to 'O' Drive, College protocol for location and sharing of data. Old hard drives disposed of or wiped by via QH	Medium (3)	Possible (2)	Medium (6)					Low	
5	Server breakdown	People: Students (potential, current & alumni), patients and the public. College business & collaborative partners	Back up Drive QH SLA, server backup system & drives - server up & running in hrs.	High (4)	Possible (2)	High (8)	Additional security drive	PR and BoG	01/06/2022		Medium	
6	Failure of Outsourced IT services: Website & SLA (IT support, hardware maintenance & daily services)	People: Students (potential, current & alumni), patients and the public. College business & collaborative partners	BoG & SMT reviews (Risk items on Agenda)	High (4)	Possible (2)	High (8)	Set up formal annual review of current SLA & maintenance contract. Set up formal annual review of website maintenance agreement (in action now)	PR and Governor	01/01/2022		Medium	

## Risk Assessment



Area	Regulation & Compliance	Date	07/02/2022	Assessment number	RC/RQ/R4
------	-------------------------	------	------------	-------------------	----------

Staff responsible	Principal	Review Date	30/06/2022
-------------------	-----------	-------------	------------

Task	GOsC - RQ Status (including impact of regulator merger or change)
------	---

Risk Number	Risk Description	Effects/ Impact on	Existing controls	Risk Rating			Further action required/ action plan	By Whom	Date	Cross reference categories	Risk with Mitigation	Update Feb 2022
				Impact (I)	Likelihood (L)	Rating						
1	Loss of RQ Status	Loss of professional recognition, ability to attract students, course validation and Ofs registration and ultimately the college business.	GOsC/QAA AMR and risk - based approach to monitoring. College RQ monitored Action Plan and monitoring with deadlines	High (4)	Unlikely (1)	Medium (4)	Monitor 2021 RQ action plan according to time frame	PR/SMT + BoG	October 2021, Dec 2021, March 2022		Low	On Track
2	GOsC Merger or New Regulator	<ul style="list-style-type: none"> <li>•New requirements for providers to meet</li> <li>•New programme requirements (not RQ)</li> <li>•New framework /amendments to standards for providers in line with other providers</li> <li>•CPD expectation changes could result in challenges to remain registered</li> <li>•Potential changes for Educators to demonstrate their ability</li> </ul>	<ul style="list-style-type: none"> <li>•PSA - overseeing health care regulators (managed process)</li> <li>Change will affect for all osteopathic providers</li> <li>•Time- managed event (legislation lengthy)</li> </ul>	Medium (3)	Possible (2)	Medium (6)	Remain updated on any current changes	PR/SMT + BoG	Ongoing		Low	

- 1 New requirements for provider to meet.  
 2 New requirements for programme to meet requirements.

Standardisation requires providers to adopt a common framework along with other professional bodies. It could lead to additional requirements for osteopaths and osteopath educators to meet to stay register. CPD challenges to complete may result in challenges for members to stay registered.

**Risk Assessment**

Low
Medium
High

Area	Regulation & Compliance	Date	07/09/2021	Assessment number	RC/V/R5
------	-------------------------	------	------------	-------------------	---------

Staff responsible	Programme Leader/Registrar	Review Date	30/06/2022
-------------------	----------------------------	-------------	------------

Task	<b>University Degree Validation (UoD)</b>
------	---

Risk Number	Risk Description	Effects/ Impact on	Existing controls	Risk Rating			Further action required/ action plan	By Whom	Date	Cross reference categories	Risk with Mitigation	Update
				Impact (I)	Likelihood (L)	Rating						
1	Non-achievement of University Validation requirements	No degree course offer & possible loss of status and therefore attractiveness of a non degree course. Effects on ability to recruit adequate numbers, college finance and business status as a going concern	Staff & College experience, partner choice, University partnership working preparation processes, student target areas for course, Validation process with conditions /action plan	High (4)	Unlikely(1)	Medium (4)		SMT			Low	
2	Loss of University Validation (College non-compliance)	As Above	University monitoring AMR, Operations Manual, Link tutor,	High (4)	Unlikely(1)	Medium (4)	None				Low	
3	Termination of Contract (either party)	As Above	MoC - terms of agreement, 'teach-out' arrangements	High (4)	Unlikely(1)	Medium (4)					Low	

Risk Assessment

Low
Medium
High

Area	Regulation & Compliance	Date	12/10/2021	Assessment number	RC/O/R6
------	-------------------------	------	------------	-------------------	---------

Staff responsible	Pr/Reg	Review Date	30/06/2022
-------------------	--------	-------------	------------

Task	OFS
------	-----

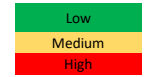
Risk Number	Risk Description	Effects/ Impact on	Existing controls	Risk Rating			Further action required/ action plan	By Whom	Date	Cross reference categories	Risk with Mitigation	Update
				Impact (I)	Likelihood (L)	Rating						
1	Failure to maintain registration compliance	College unable to attract students - no SFE loans. Loss of professional and academic credibility, impact on validation and ultimately college business Impact on registered students continuity & Progression	OFS Monitoring and checks and individual action plans. College's own governance & management and quality processes. Student Protection Plans, franchise & TO arrangements.	High (4)	Possible (2)	High (8)					Medium	

**Risk Assessment**

Area: Regulation & Compliance      Date: 12/01/2022      Assessment number: RC/SG/R 7

Staff responsible: Bursar/R      Review Date: 30/06/2022

Task: Safeguarding Vulnerable People



Risk Number	Risk Description	Effects/ Impact on	Existing controls	Risk Rating			Further action required/ action plan	By Whom	Date	Cross reference categories	Risk with Mitigation	Update Jan 22
				Impact (I)	Likelihood (L)	Rating						
1	Failure to protect patients	Loss of professional credibility, RQ/validation / OFS registration and College business	Professional body monitoring (GOsC), Use of registered practitioners, College protocols & staff training (Clinic) & monitoring of GOsC register, QRB activities, patient feedback,	High(4)	Possible(2)	High (8)	•Continue to monitor and action any changes specific to Covid 19 •Safeguarding training roll out	SMT/CLs	•ongoing	Covid RAs & Prevent RAs	Med/Low	•Continuous monitoring of COVID related factors •Safeguarding training roll out
2	Failure to protect students (including illness & mental health)	Loss of professional credibility, RQ/validation /OFS registration and College business	Recruitment protocol, Professional body monitoring (GOsC), use of registered practitioners , University screened lecturers, staff updates & training, College protocols (Clinic & lecturing), QRB activities, patient feedback,	High(4)	Possible(2)	High (8)	•Continue to monitor and action any changes specific to Covid 19. •Safeguarding training roll out	SMT/CLs	•ongoing	Covid RAs & Prevent RAs	Med/Low	•Continuous monitoring of COVID related factors •Safeguarding training roll out
3	Failure to protect vulnerable staff (include illness /mental health)	Loss of professional credibility, RQ/ OFS registration/validation and College business	Use of HR & H&S consultants, Employee Handbook with policies for H&S end HR, Professional body monitoring of staff complaints, QRB activities, recent health declaration required to ensure ability to support staff	High(4)	Possible(2)	High (8)	•Continue to monitor and action any changes specific to Covid 19 •Safeguarding training roll out	SMT/CLs	•ongoing	Covid RAs & Prevent RAs	Med/Low	•Continuous monitoring of COVID related factors •Safeguarding training roll out

Risk Assessment



Area	Regulation & Compliance	Date	10/01/2022	Assessment number	RC/P/R8
Staff responsible	Pr/ CM/HCE/B/R	Review Date	30/06/2022		
Task	<b>Prevent</b>				

Risk Number	Risk Description	Effects/ Impact on	Existing controls	Risk Rating			Further action required/ action plan	By Whom	Date	Cross reference categories	Risk with Mitigation	Update	Jan-22
				Impact (I)	Likelihood (L)	Rating							
1	<b>Leadership:</b> Leaders (including governors/trustees) within the organisation do not understand the requirements of the Prevent Duty or the risks faced by the organisation. Leaders do not understand, nor have ultimate ownership of their safeguarding processes and do not communicate and promote the importance of the duty.	<ul style="list-style-type: none"> <li>The Duty is not managed or enabled at a sufficiently senior level.</li> <li>A safeguarding culture is lacking across the institution.</li> <li>A safe environment is not provided for learners.</li> <li>The organisation does not attach sufficient priority to Prevent and risk assessment/action plans.</li> </ul>	<ul style="list-style-type: none"> <li>Prevent Duty &amp; Safeguarding training for key governors and the Senior Management Team.</li> <li>Governor identified for Prevent.</li> <li>Risk responsibility lies with governors.</li> <li>A governor is identified to oversee Risk</li> </ul>	High (4)	Possible (2)	High(8)	<ul style="list-style-type: none"> <li>Governor and SMT to monitor and sign off Prevent and vulnerable persons training by staff.</li> <li>Prevent on BoG agenda</li> <li>Increase the visual promotion of a safeguarding culture by Governors &amp; SMT presence in training &amp; discussions (BoG and Reqs meeting / student engagement forums agenda items.)</li> </ul>	<ul style="list-style-type: none"> <li>Board of Governors and SMT</li> <li>BoG</li> <li>Board of Governors and SMT</li> </ul>	<ul style="list-style-type: none"> <li>May 2021</li> <li>Aug 2021</li> <li>April 21</li> <li>June 21</li> </ul>		Medium	BoG review of training progress at August Boards 2021. Prevent on BoG agenda from 27.4.21 Prevent on student Engagement Forum from 4.5.21. when all complete re-assess LOW	BoG Items completed. Monitoring ongoing. Introduced at student forum and evidenced. AC to check ongoing engagement
2	<b>External Speakers &amp; Events: ineffective or lack of policies and procedures for external speakers or events.</b> This leads to the inappropriate interpretation of freedom of speech implications, and disproportionate application of 'Prevent' processes. Allowance of unlawful debate under the guise of freedom of speech which could leave open the potential of the hosting of prescribed organisations. No risk assessment process attached to events. Focus on events limited to on site (no consideration to partner venues or external locations.)	<ul style="list-style-type: none"> <li>ineffective external speaker and events policies/processes increases the chances of extremist infiltration through events and speaking opportunities.</li> </ul>	<ul style="list-style-type: none"> <li>Published timetable of events.</li> <li>Central office with a 'meet and greet' member of staff.</li> <li>Prevent trained senior member of staff agrees external speakers.</li> <li>External speaker identified on timetable &amp; communicated to staff &amp; students.</li> <li>Risk Assessment -standing Agenda item BoG &amp; SMT</li> <li>Freedom of speech policy published on website and intranet for students &amp; staff</li> <li>Procedure for informing and managing visitor's understanding of the College's Prevent duty expectations on campus *Lesson obs &amp; anonymous student feedback on lesson process.*</li> </ul>	Medium (3)	Possible (2)	Medium (6)					Low	Note Risks now disseminated to Sub-committees ( new structure). Chair reports back to the Board	
3	<b>Partnerships:</b> The provider does not establish effective partnerships with other partners including police, DfE FE/HE Regional Prevent Coordinator, and the local authority. Learners not engaged on Prevent duty implementation. No SPOC for Prevent-related activity. No safeguarding information sharing consideration or agreement (where appropriate) in place at the local level. No consideration given to the requirement to share appropriate information with partners.	<ul style="list-style-type: none"> <li>The organisation is not fully appraised of national and local risks</li> <li>ineffective safeguarding contacts and links, and no access to developing good practice advice or supportive peer networks.</li> </ul>	<ul style="list-style-type: none"> <li>Links with CTLP</li> <li>Links with Regional FE/HE Prevent Coordinators</li> <li>Links to the local Prevent Police.</li> <li>Links to key university partner Prevent officers &amp; policies e.g. with regards to safeguarding where space use is shared.</li> </ul>	High (4)	Unlikely (1)	Medium (4)					Low	Query - do we have links to local police? Think detail is on Policy Ask AC	
4	<b>Risk Assessment &amp; Action Plans:</b> Lack of appropriate or ineffective risk assessment related to learners or staff being drawn into terrorism. Risk assessment limited with no consideration of site, welfare, and relationships with external bodies. No update attached to Risk Assessments. Lack of policy/ procedures for managing whistleblowing and complaints.	<ul style="list-style-type: none"> <li>The provider not responding to the appropriate and level of risk hence, ineffective Prevent Management.</li> </ul>	<ul style="list-style-type: none"> <li>Risk assessments with action plans with time frame and person responsible identified</li> <li>Risk Assessments monitored up to Board level.</li> <li>Risk Assessments have updates &amp; an annual review date</li> <li>Risk Assessments published</li> <li>Adaptable Risk Management process.*</li> <li>Whistleblowing &amp; complaints policies</li> </ul>	High (4)	Possible (2)	High (8)					Low	Yes	



5	<p><b>Staff Training</b> : Appropriate staff/governors not trained and unaware what extremism is and radicalisation means and why people may be vulnerable. Appropriate staff uninformed on Prevent measures and actions and behaviours to look out for and how to make a referral, including Channel. Appropriate Staff and governors do not undertake the appropriate level of training. Lack of knowledge prevents the identification of vulnerabilities that may be exploited by extremist narratives. Volunteers and subcontractors not included in any training plans.</p>	<p>•Staff do not recognise behavioural signs of radicalisation and vulnerabilities. •The risk of harm is not reported properly and promptly by staff.</p>	<p>•Schedule of Prevent training for staff at all levels •Monitored record of staff Prevent training from Board to key front facing staff in contact with students, patients and the public •Key contractors on the training schedule •Regular visitors informed of Prevent expectations via a briefing document.</p>	High(4)	Possible (2)	High (8)				(cross ref 2)	Low		Training is ongoing. See link with Safeguarding
6	<p><b>Welfare &amp; Pastoral Support</b>: Vulnerabilities are not addressed appropriately and lead to potential radicalisation or safeguarding issues. Insufficient appropriate pastoral and welfare support available to all students. Ineffective policies in place regarding the use and management of identified faith space including detailing the procedure for managing any issues that arise with the use of the area.</p>	<p>•Learner vulnerabilities are not appropriately addressed resulting in potential for radicalisation. •Prayer and faithspace inappropriately utilised or managed and used and therefore facilitates extremist action. •Inappropriate management of the faith facilities could result in tensions and a lack of learner cohesion.</p>	<p>•Cross college pastoral support and key area and academic level support tutors •Annual declaration and fitness to practice monitoring process •Identified faith spaces on campus</p>	High (4)	Possible (2)	High(8)	•Identify faith space on partner campus's used at the weekends	•Prevent Officer	• May 2021		Low	ID outstanding Partner Faith spaces, but still assess as Low	Faith Space Identified on College and Partner campuses
7	<p><b>Safeguarding</b>: Safeguarding leads are unaware of the links between vulnerabilities and radicalisation. Safeguarding leads are not aware of the Channel process, nor how to refer to it. Prevent is not embedded within the safeguarding policy and within the culture of safeguarding culture within the institution. Radicalisation and related vulnerabilities are not referred to within safeguarding training which leaves staff with a knowledge gap and the risk to not be recognised. The internal safeguarding referral process does not mention Prevent.</p>	<p>•Learner vulnerabilities are not appropriately addressed resulting in potential for radicalisation. •Staff are unsure how to recognise or refer a Prevent concern and see no link to Safeguarding, leaving vulnerabilities unmitigated.</p>	<p>•Safeguarding leads identified and trained across The College. •Prevent embedded into Safeguarding Policy •Safeguarding training for key staff including Board members</p>	High (4)	Possible (2)	High (8)	•Continued roll out of Safeguarding training for key staff including Board members	SMT & LMs	From March 2021 & Ongoing	(cross ref 1) & Vul people RAs (1 - 3)	Medium	see 1 re monitoring training roll out. When complete assess as LOW	Ongoing and included as part of expected training for new staff
8	<p><b>IT Policies</b>: Learners can access terrorist and extremist material when accessing the internet at the institution. Learners may distribute extremist material using the institution IT system. Unclear linkages between IT policy and the Prevent duty. No consideration of filtering as a means of restricting access to harmful content.</p>	<p>•Ineffective IT policies increases the likelihood of learners and staff being drawn into extremist material and narratives online. •Inappropriate internet use by learners is not identified or followed up.</p>	<p>IT policies in place for staff in employee handbook &amp; available for contractors</p>	High (4)	Possible (2)	High (8)	•Update IT policy & make reflective of IT use on campus •Link IT policy and Prevent duty by promoting to students & staff e.g. the Phone App (i-Report It), to report suspect websites. •Block and monitor access inappropriate websites	•Pr/PO	June 2021		Medium	updated IT Policy scheduled for BoG 27.4.21. IT consultants contacted. Solution proposed to upgrade monitoring & blocking to go to FSC 11.5.21. When complete Assess as LOW	Completed. Further updates & Acceptable Use Policy developed and to Jan 22 Board. Increased dependence on IT keeps this as medium. Discussions moving forward on system upgrades for future.
9	<p><b>Building Learners Resilience to radicalisation via the environment and Curriculum</b>: The setting does not promote the development of appropriate values and community cohesion. Appropriate values are not exemplified by staff to learners, that safeguard against radicalisation and terrorism. The setting exposes learners to intolerance to others.</p>	<p>•The risk is learners are exposed to intolerant or hateful narratives and lack understanding of the risks posed by terrorist organisations and extremist ideologies that underpin them. •A risk of learners holding intolerant views and creating tensions both within the institution and the community.</p>	<p>• Codes of conduct for all staff (teaching and non-teaching staff) •The institution carries out recruitment checks on all staff. •Classroom teaching is monitored by senior leaders through observations, text &amp; content checks (quality assured). •The institution provides opportunities within the curriculum to discuss controversial issues and for pupils to develop critical thinking and media literacy skills.</p>	High (4)	Unlikely (1)	Medium (4)					Low		Yes