Prevent Policy and Procedures

Table of Contents

1. Introduction 3
2. Purpose and scope of the policy and procedures 3
3. Legislative requirements 3
4. Management and oversight of the Prevent Duty 4
   - 4.1 Senior management 5
   - 4.2 Prevent Duty Task Team ..... **Error! Bookmark not defined.**
   - 4.3 Governance oversight 6
   - 4.4 Partnership 6
   - 4.5 Engagement with students 7
   - 4.6 External speakers and events 7
5. Risk Assessments 8
   - 5.1 Initial risk assessment 8
   - 5.2 Annual and ad-hoc risk assessments 8
6. Prevent Duty Procedures 9
   - 6.1 Staff Training 9
   - 6.2 Welfare Support for Students 10
   - 6.3 Confidentiality, Information Sharing and Record Keeping 11
   - 6.4 Information Technology System and Measures 13
   - 6.5 Monitoring and Reporting 14
7. Related documents 14
8. Definitions 15
9. Accountabilities 16

1. Introduction

1.1 Introduced under the Counter-Terrorism and Security Act 2015, the Prevent Duty requires universities to take appropriate steps to prevent people being drawn into terrorism. As part of its role safeguarding and supporting students and staff, the Engineering College of Technology (ECT) has a statutory responsibility applicable to 'Specified Authorities' under the Act.

1.2 ECT recognises that it has an important role in preventing people from being drawn into terrorism, including violent extremism and non-violent extremism, which can create an atmosphere conducive to terrorism and can popularise views which terrorists may exploit.

2. Purpose and scope of the policy and procedures

2.1 The purpose of this policy and procedures is to fulfil its responsibility relating to Prevent Duty by reducing the threat to the UK from terrorism by stopping people becoming terrorists or supporting terrorism, or being exposed to incitement to extremism or radicalisation by ensuring that measures are in place to:

- Ensure that ECT exercises its legal responsibilities relating to Prevent Duty
- The management and the Governance Board oversight over ECT's Prevent Duty
- The role of the Prevent Duty Task Team
- Adherence by the partnership institution
- Engagement with students through the Student Council and briefing of students on their and ECT's responsibilities relating to Prevent Duty
- Conducting initial, annual and ad-hoc risk assessments
- The Prevent Duty procedures relating to staff training, welfare support for students, confidentiality, information sharing and record keeping, ECT's Information Technology system and measures, as well as monitoring and reporting.

2.2 This document is not directed at any specific religion, religious group or at the proponents of any other set of beliefs, and does not discriminate against any religion, group or individuals based on their particular personal characteristics, such as ethnicity, place of origin, language, religion or beliefs. Its principal aim is to ensure that ECT is able to monitor, manage and deal effectively in meeting its obligations in relation to its Prevent Duty.

3. Legislative requirements

3.1 The policy and procedures will ensure that ECT's policies, procedures and practices are aligned with the requirements and guidelines in the following documents:

- Counter-Terrorism and Security Act 2015 (https://www.legislation.gov.uk/ukpga/2015/6/contents)
- Prevent duty guidance: Guidance for specified authorities in England and Wales (https://www.gov.uk/government/publications/prevent-duty-guidance)
- Consumer Rights Act 2015: Consumer Rights Act 2015 (legislation.gov.uk)
- Data Protection Act 2018: Data Protection Act 2018 (legislation.gov.uk)
- Equality Act 2010: https://www.gov.uk/guidance/equality-act-2010-guidance#equalities-act-2010-legislation

- Higher education: consumer law advice for providers – helping you comply with your obligations (CMA182) of the Competitions and Market Authority: Higher education: consumer law advice for providers - GOV.UK (www.gov.uk)
- Terrorism Act 2000 (https://www.legislation.gov.uk/ukpga/2000/11/contents)
- The good practice framework: handling student complaints and academic appeals of the Office of the Independent Adjudicator for Higher Education (OIA), December 2022 (www.oiahe.org.uk/good-practice-framework.aspx).
- UK General Data Protection Regulation (UK GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (United Kingdom General Data Protection Regulation)(Text with EEA relevance) (legislation.gov.uk)

4 Operation of the Prevent Duty

Responsibilities

4.1 The Prevent Lead for the policy and procedures is the Head of Academics and Operations The Prevent Lead acts as the Single Point of Contact (SPOC) for engagement with external agencies. The Deputy Prevent Lead is the Compliance and Risk Manager. The Prevent Lead Chairs the Prevent Duty Task Team with responsibility for developing a Prevent Duty Action Plan. All concerns relating to Prevent raised by students are staff are received by the Prevent Lead.

4.2 The Prevent Task Team is made up of the Head of Academics and Operations (Prevent Lead), Compliance and Risk Manager (Deputy Prevent Lead), Data Protection nominee, and a Student Support senior post holder.

4.3 The Chair of the Governance Board engages with the Head of Academics and Operations to approve and monitor the implementation of the Prevent Duty Action Plan.

Raising a concern and making responses

4.4 The following table shows the steps taken in raising a concern and making responses:

A. Identify & report:	Any student or staff member can raise a concern
	All actual or suspected incidents of terrorism, extremism or radicalisation or incitement towards terrorism, extremism or radicalisation must be reported verbally and/or in writing to the Head of Academics and Operations, Chair of the Prevent Duty Task Team.
B. Triage & fact-finding:	Deputy Prevent Lead gathers proportionate information and records the case.
C.	Prevent Lead convenes a meeting of the Prevent Task Team

Prevent Panel (as required):	Upon receiving information on an actual or suspected threat, the Task Team will immediately meet to conduct a risk assessment and develop a Prevent Duty Action Plan (PDAP).
	In cases where external support is required, the Head of Academic and Operations will engage with the Regional Prevent Education Co-ordinators (RPEC) for assistance in implementing the PDAP.
D. Decision & Actions:	In cases where urgent action is required, the Head of Academics and Operations will communicate directly with the Chair of the Governance Board who could decide on behalf of the Board the steps to be taken.
	The Head of Academics and Operations will share the report and PDAP with the senior management team and any ECT full-time and part-time staff who may be directly or indirectly involved or affected by specific incidents.
	The Head of Academics and Operations will table the report and PDAP at the next Governance Board meeting. The Chair may take appropriate action if circumstances necessitate. A report will be prepared for Academic Board.
	Available decisions are: No further action; Internal support plan (review date set); External referral (Regional Prevent Coordinator or Police if immediate safety/criminal threshold met.)
E. Record-keeping:	Decisions and their rationale are recorded. Minimal data is shared externally on a need-to-know basis. Records are retained as per the ECT Record Retention schedule.
	An annual report on the Prevent Policy and actions taken will be prepared and considered by Academic Board and the Governance Board. This will be prepared by the Compliance and Risk Manager and presented by the Prevent Lead.
	The Head of Academics and Operations is the single point of external contact (SPOC) for the implementation of the Prevent Policy and Procedures. The SPOC will engage with the designated Regional FE/HE Prevent Co-ordinator for guidance and assistance whenever the need arises.

Management of Prevent

4.5 The Head of Academics and Operations is the single point of contact (SPOC) for the implementation of the *Prevent Policy and Procedures*, supported by members of the senior management team. The Head of Academics and Operations will establish, and Chair, a Prevent Duty Task Team (see 4.1). This Task Team is responsible for driving the implementation of this policy and procedures, and monitoring compliance to it.

4.6 The Head of Academics and Operations will establish contact with the Regional FE/HE Prevent Co-ordinators and engage with the designated coordinator for guidance and assistance, when the need arises.

4.7 The Prevent Lead (supported by the Deputy) will engage externally, maintain active liaison with the Regional Prevent Coordinator, Local Authority and Police and participate in sector briefings to keep ECT current on threat-level updates and good practice. The Prevent Lead will communicate risk updates by cascading relevant threat-level and policy updates to ECT managers, staff and partners promptly.

4.8 The Deputy Prevent Lead will ensure that staff are trained to an appropriate level and that skills are refreshed. Appropriate assurance is provided on training that has been delivered to the Academic Board and the Governance Board.

4.9 Appropriate reports are prepared for the Academic Board and the Governance Board. The Lead will also ensure that related policies are aligned with statutory guidance. The Lead will provide termly assurance to the Governance Board. They will prepare for the annual OfS ADR readiness and sign-off providing evidence of training, welfare cases, on-line events and external speaker activities and details of referrals made for investigation.

Governance oversight

4.10 The Governance Board will exercise competent governance oversight of and accountability for ECT's responsibilities relating to Prevent Duty in its review of all ECT reports relating to Prevent Duty. The Board will provide strategic direction to ECT's management on compliance to legal requirements and the review and continuous improvement of this policy and procedures, and related matters.

4.11 The Chair of the Governance Board will communicate all decisions made on behalf of the Board to the other members of the Board, and table all related decisions at the next Board meeting for approval. Both the Governance Board and the Academic Board could make recommendations on improvements to the execution of ECT's Prevent Duty.

4.12 ECT designates the Accountable Officer (AO) for OfS purposes as the Head of Academics and Operations. The AO is responsible for ensuring ECT meets its Prevent duty reporting requirements, including completion and submission of the Prevent Accountability and Data Return (ADR) by the OfS deadline each year, and for providing any additional information reasonably required by OfS. The Governance Board will receive the draft ADR for approval prior to submission, and a post-submission assurance report noting actions arising.

4.13 ECT notifies the OfS within five days of any material change affecting Prevent delivery (e.g., Prevent Lead change; core policy changes; new campus; delivery model changes). Updated policies are uploaded where relevant.

Partnerships

4.14 The Head of Academics and Operations will ensure that ECT's Australian-based sister organisation, the Engineering Institute of Technology (EIT), is informed of this policy and procedures. Furthermore, the Head of Academics and Operations will inform EIT's Head of Higher Education and Global Strategy of all matters relating to *Prevent Policy and Procedures* that are relevant to EIT, particularly in the support it will be providing to ECT during its first year or operation as stipulated in ECT's *Student Protection Plan,* and of its responsibility to disclose any relevant information to the ECT.

Engagement with students

4.15 The Student Council, that will be established once the first cohort of students is enrolled, will be the main forum for student participation in ECT's academic structures, in accordance with *Terms of Reference - Student Council*. The briefing during the induction of members of the Council will include an overview of this policy and procedures as part of the explanation of the Council's role.

4.16 During compulsory induction, enrolled students will receive relevant information on ECT's Prevent Duty to ensure that they understand their responsibilities in promoting a safe educational environment, together with information on policies and procedures that are particularly relevant to students. They will also be warned of the consequences of accessing, sharing or placing on ECT's IT system inappropriate material relating to extremism, radicalisation or terrorism.

4.17 Students will be able to make use of the Student Council and the student representative on the Academic Board to raise concerns and request improvements in any matters relating to ECT's Prevent Duty. They will have an opportunity to participate in an annual review of the policy.

4.18 Individual students who have complaints or concerns relating to ECT's exercise of its Prevent Duty can raise their concerns in accordance with the *Student Complaints Policy* and *Procedures.*

4.19 Students will be informed that they have the right to engage directly with the Head of Academics and Operations if they have concerns about matters relating to terrorism or extremism. They also have the right to liaise with appropriate external agencies, such as the Regional Prevent Coordinator Channel.. They may report issues to the Police at any stage of the process if they are not satisfied that their concerns have been addressed.

External speakers and events

4.20 ECT takes reasonable and practicable steps to secure freedom of speech within the law for visiting speakers and others. Decisions, mitigations or conditions are documented with explicit regard to the free speech duties and may not be based on a speaker's ideas or opinions.

4.21 ECT lecturers and staff are primarily responsible for the online delivery of its programmes, with some involvement of external speakers or external events. If the need would arise for external speakers or events, the Head of Academics and Operations will ensure that all external persons involved are fully briefed on the Prevent policy and procedures. ECT will also inform them of ECT's policies on Academic Freedom, Ethics, Integrity and Honesty and its commitment to the principles of free intellectual enquiry, free expression and freedom of speech within the law. Organisers will complete a proportionate risk assessment covering topic, speaker background, format and chat/interaction controls. On-line chats may be moderated. Streaming may be time-delayed. Where concerns arise, events may be postponed or conditions applied to proceed.

4.22 Before any online event with an external contributor, organisers complete a short risk checklist (topic sensitivity; speaker background; format & chat controls; moderation; time-delay if needed; recording; attendee management). Decisions and mitigations are logged**;** lawful freedom of speech and academic freedom are protected. A short risk assessment checklist will be made available.

4.23 The Terrorism (Protection of Premises) Act 2025 ("Martyn's Law") will be enacted as this policy is published. Where ECT controls any in-person premises or events (e.g., graduations, assessments, conferences etc), we will assess whether they fall within the Act's scope and, if so, implement the required protective measures and staff awareness accordingly.

5 Risk Assessments

Initial risk assessment

5.1 Risk assessment occurs before student recruitment and then annually. ECT will conduct an initial risk assessment to assess where and how their students and staff might be at risk. This risk will also cover a range of institutional policies and procedures relating specifically to the online delivery of ECT's programmes. The findings from the initial risk assessment will inform the Prevent Duty Action Plan that will be appropriate for the ECT context, the online delivery model, and the requirements outlined in the Prevent Duty statutory guidance.

5.2 The preliminary risk assessment indicated the following potential risks to ECT staff and enrolled students:

- External factors: Students/staff exposed to unauthorised extremist views at ECT, rallies or demonstrations in or around the premises and staff/students becoming radicalised via off campus methods.
- IT factors: Students and staff accessing or placing inappropriate material on ECT's IT systems
- ECT premises: The risk of students/staff producing or reading posters or materials of an inappropriate nature on or around ECT's premises or the risk of external persons on the premises.
- On-line delivery specific risk indicators include:
  (i) off-platform communities used for course collaboration;
  (ii) livestreamed sessions and interactive chat;
  (iii) sharing of extremist content links via VLE tools;
  (iv) impersonation/doxxing;
  (v) targeted harassment of staff/students.

5.3 ECT will respond to instances of significant platform changes and spikes in keyword-flagged incidents.

Annual and ad-hoc risk assessments

5.4 The Prevent Duty Task Team will conduct risk assessments relating to Prevent Duty in accordance with ECT's *Risk Management Policy*, to identify vulnerabilities within the student body, staff and the community at large. Risk assessments will be conducted annually as part of ECT's overall risk assessment strategy. Ad-hoc risk assessments will be conducted upon receiving information on an actual or suspected threat.

5.5 Risk assessment and case-handling focus on behaviours and vulnerability indicators, not on nationality, religion, ethnicity or other protected characteristics. Staff must avoid assumptions and ensure decisions are proportionate and evidence led.

5.6 The Team will consider the likelihood of the risk occurring (from very low to very high) and impact of the risk occurring (from insignificant to extreme). The key risks will be

recorded in the *Risk Management Register*, and a Prevent Duty Action Plan will be developed on how to deal with the risks.

5.7 The following are examples of potential risks related to terrorism and extremism:

- Radicalisation of students who may be influenced by extremist ideologies, which can include both violent and non-violent extremism
- Online radicalisation, particularly in view of the online delivery of ECT's programmes
- Specific student groups may be more susceptible, for example students living in or from countries with a high prevalence of terrorism
- Threats to freedom of speech aimed at preventing staff and students from sharing their views and experiences and allowing them to challenge and interrogate different viewpoints in a thoughtful, tolerant and courteous way
- External factors, such as students/staff being exposed to unauthorised extremist views at rallies, demonstrations or posters in or around ECT's premises or at external premises
- Students/staff accessing or placing inappropriate material on ECT's IT systems, such as Moodle, which is used as the Virtual Learning Environment or BigBlueButton video-conferencing software.
- Inadequate staff awareness and training to recognise signs of radicalisation.

6 Prevent Duty Procedures

Staff Training

6.1 All staff will receive induction training in Prevent Duty, as part of the training on ECT's responsibilities in terms of UK legislation applicable to higher education institutions. The aim of the training will be to enable all managers and staff to understand the ECT's Prevent Duty and their own responsibility in safeguarding students from terrorism, extremism or radicalisation. The Learning Support Officers and other support staff, teachers and the Prevent Duty Task Team will receive more extensive training relating to the nature of their work and function in addressing Prevent issues.

6.2 The Head of Academics and Operations is responsible for developing a training plan that describes the initial and subsequent training for all staff and the training customised for different staff. The plan will include refresher briefings at least annually. The training of management and staff will focus on:

- Understanding their duties and responsibilities in relation to ECT's Prevent Duty
- Understanding the role of the Task Team in conducting risk assessments
- Identifying the risks and signals of radicalisation and extremism and potential affiliation with terrorism and ECT's responses to addressing these
- Understanding the referral procedure and what to do with the information they have
- Understanding the need for confidentiality and support available to students and staff who have been subjected to such risks
- Understanding the consequences of staff/students accessing, sharing or placing on ECT's IT system inappropriate material relating to extremism, radicalisation or terrorism

- Recognising the need to balance ECT's obligations under the Prevent Duty with commitments to academic freedom and freedom of expression as stipulated in its Regulations on Academic Freedom, Ethics, Integrity and Honesty

6.3 In addition to the above, the Task Team will be trained in:

- Understanding ECT's Prevent Duty to undertake risk assessments and action planning
- Conducting risk assessments in according to ECT's *Risk Management Policy* and in adherence to other internal and regulatory requirement
- Developing a Prevent Duty Action Plan that is proportionate and institution specific, consistent with its ethos and values, based on the findings of a risk assessment
- Applying sound principles of risk assessment in assessing the risk of extremism, radicalisation and terrorism in the ECT context with a focus on behaviours and vulnerability indicators, rather than nationality, religion, ethnicity or other protected characteristics.
- Ensuring that decisions made are proportionate and evidence-based.
- Understanding the support and advice available from external agencies.
- Understanding of risk assessment

6.4 ECT will use the e-learning module and other learning resources that are available nationally and locally for higher education institutions and add these to its Virtual Learning Environment where permitted. ECT will also engage with the local Prevent Coordinator to access workshops, training sessions and resources for its staff across different sectors to raise awareness about the Prevent Duty.

6.5 ECT staff will also be informed that they should engage directly with the Compliance and Risk Manager if they have concerns about matters relating to terrorism, extremism or radicalisation. They also have the right to liaise with appropriate external agencies, such as the Regional Prevent Coordinator, Channel and the Police if they are not satisfied that internal processes have addressed their concerns.

6.6 Training effectiveness is evaluated annually.

6.7 The arrangements for mandatory training can be summarised as follows:

Mandatory training and refreshers

- All staff complete Prevent e-learning within 1 month of start and every 2 years thereafter.
- Student-facing staff, case-handlers and managers complete annual refresher + short assessment/quiz.
- Completion is tracked by HR/L&D; non-completion triggers reminders and line-manager escalation.
- Training stresses proportionality, academic freedom, online-delivery risks, information-sharing and data protection.

Welfare Support for Students

6.8 ECT will establish and maintain an effective welfare support system to create an environment where students feel safe and supported and to ensure that individuals at risk can receive appropriate support. Learning Support Officers may support students

by referring them for external specialised services for counselling, medical, welfare or legal support services, or support from a religious institution

6.9 The welfare support to students will be provided in accordance with ECT's *Student Support Policy* and *Procedures*. These ensure that adequate support is provided to meet student needs.

6.10 ECT has developed a Safeguarding policy that is concerned with supporting students that are vulnerable. Robust safeguarding policies are in place to ensure that those at risk of radicalisation are identified and appropriate support is provided. Students or staff raise concerns regarding radicalisation internally with the Compliance and Risk Manager. This may be done in person, by completing a form to be emailed, via a form on a portal on the VLE or by an anonymous notification 'button' on the website. A link to the Prevent national referral form is provided on the web site, the VLE and the programme handbook.. These policies and procedures help ECT to satisfy itself that it is able to identify and support people affected by radicalisation.

6.11 The Head of Academics and Operations, as the accountable manager and single point of contact for the implementation of the *Prevent Policy and Procedures*, will ensure that support is provided for staff and students that may be affected by exposure to actual or potential acts of radicalisation, extremism or terrorism. Support may be provided from within ECT or by signposting to external agencies and will be coordinated by the Compliance and Risk Manager.

6.12 The Head of Academics and Operations may engage with the Regional Prevent Coordinator, the Police, other local authorities and relevant agencies. Where there are concerns about an individual's vulnerability or exposures to radicalisation, extremism or terrorism, the Head of Academics and Operations will refer students and staff for appropriate external support, which could include, but are not limited to the following interventions:

- Referral to the Regional Prevent Coordinator responsible for coordinating Prevent-related activities and support.
- Referral to the Channel programme, a non-governmental organisation for tailored support through a multi-agency approach to developing a support plan based on the individual's needs (https://www.gov.uk/government/publications/channel-and-prevent-multi-agency-panel-pmap-guidance)
- Referral to a relevant faced-based institution for pastoral or spiritual support

6.13 Many students study outside the UK. While the Prevent Duty applies in the UK, we will support students wherever they are, so far as possible and where an external referral is appropriate liaise primarily with the Regional Prevent Coordinator as our single UK point of contact.

Confidentiality, Information Sharing and Record Keeping

6.14 Confidential records are kept in line with ECT's Data Protection and Record Retention policies; access is restricted to authorised staff.

6.15 When seeking to share personal data regarding people susceptible to radicalisation, the Head of Academics and Operations will consider whether it is appropriate to rely on securing the person's consent when complying with the requirements of data

protection legislation. Where it is not possible to obtain consent, it is still possible to share information internally and externally if there is a lawful basis for doing so.

6.16 ECT will only process personal data for the legitimate purposes for which it was obtained in the execution of processes relating to teaching and learning, and related administrative processes. This will be in accordance with the *Data Protection Policy and Procedures*, that stipulates that personal data should be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

6.17 All the records relating to radicalisation, extremism and terrorism will be separated from other student/staff records and secured with access codes that are restricted to those who need access to perform functions relating to ECT's Prevent Duty. Where feasible, the privacy will be protected through data minimisation (e.g. anonymisation).

6.18 ECT recognises that the nature of the work undertaken in supporting students and staff may result in the disclosure of specific information about an individual or a group of individuals involved in unlawful activities. In accordance with the law, such information can be disclosed to external entities, including the Prevent Coordinator and the police.

6.19 ECT will securely store all records containing personal data and take all reasonable security measures to protect such data from loss, interference, unauthorised access, misuse, modification or disclosure. This is ensured via storage of records in hard copy form in lockable cabinets as well as by rigorously restricting access to electronic records to selected authorised staff members. ECT will establish, maintain and continuously upgrade a set of robust and best-practice security mechanisms to protect its information technology infrastructure and electronic records.

6.20 Processes for ensuring the security, integrity and confidentiality of personal data will be performed in accordance with ECT's *Digital Teaching and IT Acceptable Use Policy*, which includes the following prescripts:

- Access of managers, staff and others working with or performing work on behalf of ECT will be restricted to personal data that they need to know and are authorised to use for the performance of their specific job functions. Additional restrictions are placed on the access to sensitive data to designated managers only
- Where elevated access is granted to personal data, this must be consistent with an individual's roles and responsibilities, and they must take all reasonable measures to protect the confidentiality, integrity, and availability of personal data.
- Encryption and password-protection will be used to restrict access to all personal data.

6.21 The Head of Academics and Operations as Accountable Officer, reports Prevent-related serious incidents via the OfS portal as a reportable event within five days of identification. Personal data is not supplied to OfS unless requested. Near misses are reported when they would have impacted Prevent implementation had they progressed.

Information Technology System and Measures

6.22 Guidance for students and staff on the appropriate use of IT equipment and networks, is provided with specific reference to the Prevent duty is contained in the *Digital Teaching and IT Acceptable Use Policy*. This is also provided in the programme handbook.

6.23 ECT is committed to maintaining a secure IT environment by proactively identifying potential risks and implementing robust measures to combat threats. These potential risks include unauthorised access, data breaches, cyber-attacks, as well as the posting of unwarranted content relating to terrorism, extremism and radicalisation. ECT operates risk-based monitoring of institutional platforms (VLE, video-conferencing, collaboration tools) to detect and respond to content that may indicate a Prevent risk. Monitoring focuses on institutional accounts and spaces used for teaching/learning; it does not extend to personal devices or private accounts. Filters/alerts are reviewed at least annually for effectiveness and unintended bias. Where automated tools flag content, human review confirms context before any action is taken.

6.24 ECT will maintain a robust Information Technology System to protect the integrity, confidentiality and security of all information, processes and activities in accordance with its *Digital Teaching and IT Acceptable Use Policy.* ECT's IT system will be continuously monitored, evaluated and continuously upgraded to ensure that it adheres to all legal requirements relating to Prevent Duty in terms of the Counter-Terrorism and Security Act 2015, as well as those relating to consumer rights and data protection.

6.25 ECT will continuously conduct network monitoring and system audits, coupled with advanced security protocols to effectively respond to threats before they evolve into critical issues. ECT will employ stringent measures to restrict access control specifically against these threats, such as multi-factor authentication and complex password protocols to safeguard both physical and remote access to crucial systems to prevent access by unauthorised individuals.

6.26 ECT will establish and maintain sophisticated protocols for the timely detection of potential security vulnerabilities, involving routine inspections of login attempts, and audit logs, and deploying real-time alerts for any abnormal activities, followed by the prompt removal of any threatening, offensive, or unwarranted information within the IT system.

6.27 In the event of incident risks, ECT will, as a matter of urgency, proactively update security protocols based on insights gained to maintain a robust IT infrastructure, adept at adapting and recovering from potential security incidents, and minimising future risks, thereby safeguarding the confidentiality, integrity, and availability of information.

6.28 ECT applies proportionate, risk-based monitoring of institutional platforms (e.g., VLE forums/DMs, blogs, live-chat) focused on ECT-managed spaces only. Automated keyword screening generates regular reports for the Prevent Lead/Deputy to review, with human confirmation of context before any action. Students are informed of the arrangements for monitoring via the Terms & Conditions/Handbook**.** Filters/alerts are reviewed annually for effectiveness and unintended bias.

6.29 An explanation of how filtering/monitoring is applied is provided for students. The policy on retention of information is explained. Processes for the review of logs is

explained and assurance that no action is taken without human review is provided. Limits are explained (e.g., personal devices on mobile networks) and align the control methods taken to risk (e.g. Bring Your Own Device (BYOD)/guest Wi-Fi). Students will be informed that there will be an annual effectiveness and bias review.

Monitoring and Reporting

6.30 The Teaching, Learning and Quality Committee, appointed by the Academic Board, will be mainly responsible for the continuous monitoring and evaluation of the implementation of the *Prevent Policy and Procedures*. The Committee's responsibilities include the following during its monthly meetings:

- Reviewing the reports of the Prevent Duty Task Team, as well as any information or complaints received from students/staff that were not investigated by the Task Team
- Monitoring progress on the implementation of the Prevent Duty Action Plan
- Monitoring adherence to the Prevent Policy and Procedures
- Monitoring the implementation of the Prevent Duty Action Plan
- Recommending improvements to the Policy and Procedures, and the Prevent Duty Action Plan
- Submitting quarterly monitoring reports to the Governance Board for approval and to the Academic Board for noting.
- Preparing an annual evaluation of training impact and an Accountability and Data Return (ADR) readiness check each autumn detailing evidence sources and signatories in line with the OfS submission deadline.

6.31 The following annual timeline will normally apply:

- September–October: evidence collation and ADR readiness check (training completion rates; welfare/support cases; online event/speaker decisions; number of concerns/referrals; monitoring review log).
- November: Governance Board review/sign-off of the ADR.
- By OfS deadline, submit ADR.
- Provide a post-submission assurance report to Governance Board with actions confirmed.

7 Related documents

7.1 This policy and procedures should be read in conjunction with the following ECT documents:

- ECT's Prevent Duty Risk Assessment
- ECT's Prevent Duty Action Plan
- ECT's initial Prevent Duty Risk Assessment
- ECT's annual updated Prevent Duty Risk Assessments.

7.2 The policy and procedures have been written to support the following ECT documents:

- Academic Honesty and Misconduct Policy and Procedures
- Code of Ethics
- Consumer Protection Policy and Procedures

- Equality, Diversity and Inclusion Strategy
- Data Protection Policy and Procedures
- IT Policy for Systems Administrators and Managers
- ECT's Regulations on Academic Freedom, Ethics, Integrity and Honesty
- Risk Management Policy
- Student Code of Conduct.

7.3 ECT will maintain a public web page with Prevent principles, named Prevent contacts, an anonymous/named report form, links to free-speech and student conduct policies and emergency guidance.

8 Definitions

Channel: A national non-governmental programme designed to support individuals who may be vulnerable to recruitment by violent extremists, which involves a multi-agency approach that provides tailored support aimed at diverting individuals from radicalisation.

Due Regard: A legal standard requiring authorities to consider the need to prevent individuals from being drawn into terrorism when carrying out their functions, ensuring that this consideration is integrated into their operational practices.

Extremism: The vocal or active opposition to fundamental British values, which include democracy, the rule of law, individual liberty, and mutual respect and tolerance for different faiths and beliefs. Extremism can manifest in both violent and non-violent forms and could include calls for the death of members of our armed forces, whether inside this country or in another country.

Interventions: Programmes intended to divert individuals from engaging in terrorist activities, which could include mentoring, counselling, pastoral or spiritual support, and community engagement initiatives aimed at fostering resilience against extremist ideologies.

Prevent. In the context of Prevent Duty, it refers to actions to stop people becoming terrorists or supporting terrorism, and safeguarding them from extremism and radicalisation.

Prevent Duty: A legal obligation in terms of the Counter Terrorism and Security Act 2015 requiring "specified authorities", which include educational institutions, to have "due regard to the need to prevent people from being drawn into terrorism" as part of their normal functions.

Radicalisation: The process through which an individual comes to support extremist ideologies and potentially engage in terrorist activities, and which could be influenced by various factors, including personal experiences and social environments.

Terrorism: In terms of the Terrorism Act 2000, terrorism includes:

- The use or threat of specific action that involves serious violence against a person, involves serious damage to property, endangers a person's life (other than that of the person committing the action), creates a serious risk to the health or safety of the public or a section of the public, is designed seriously to interfere with or seriously disrupt an electronic system.
- The use or threat is designed to influence the government or an international governmental organisation, or to intimidate the public or a section of the public.
- The use or threat is made for the purpose of advancing a political, religious, racial, or ideological cause.

Safeguarding: The broader process of protecting susceptible individuals from harm from terrorism-relating incidents, which includes safeguarding against extremism and radicalisation alongside other forms of abuse or exploitation.

9 Accountabilities

9.1 The Governance Board is responsible for review and approval of this policy and procedures. The policy and procedures are to be implemented via induction and training of staff and distribution to students and ECT's community via the website and other publications.

Document Control	
Document title	Prevent Policy and Procedures
Version no.	1.2
Date Approved	TBC
Approving Body	Governance Board
Policy Custodian	Dean
Policy Contact	Quality and Compliance Manager
Commencement Date	*Not yet available*
Review Period	Annually
Next Review Date	*Subject to the commencement date*
Related documents	• Academic Honesty and Misconduct Policy • Academic Regulations Manual • Consumer Protection Policy and Procedures • Data Protection Policy and Procedures • Equality, Diversity and Inclusion Strategy • IT Policy for Systems Administrators and Managers • Risk Management Policy • Student Complaints, Grievances and Appeals Policy • Student Complaints, Grievances and Appeals Procedures • Student Protection Plan • Student Support Policy • Student Support Procedures

Revision History		
Version	**Date**	**Description of key changes**
1.1	Nov 2024	New document developed to meet the requirements for higher education institutions relating to Prevent Duty
1.2	Aug 2025	Updated in line with DFE and OfS updates
1.3	Nov 2025	Further alignment with OfS requirements