Radicalism, Extremism & Terrorism Organisations Policy

PRN-163: Radicalism, Extremism & Terrorism Organisations Policy
Company Name: AI Auto-Tech Ltd
Trading/Business Name: CAREHOPES
Company Registration Number: 15556946
SIC Code: 88100 – Social Work Activities Without Accommodation for the Elderly and Disabled
Email: admin@carehopes.com
Version Number: V01 20260815
Date of Review: (August 2026)

---

1. Policy Statement

CAREHOPES (TC) is committed to operating ethically, lawfully, and in alignment with UK and international counter-terrorism standards. TC will **not partner, transact, donate to, sponsor, or engage with any individual, group, or organisation that is proscribed, designated, or publicly known to support, promote, finance, or engage in radicalism, extremism, or terrorism**.

TC adopts a **zero-tolerance approach** to any form of extremist ideology or terrorism-related activity. This includes organisations listed by:

- UK Home Office Proscribed Terrorist Organisations List
- United Nations Security Council Sanctions List
- European Union Terrorist List
- Other recognised international authorities

TC will not support, sponsor, or facilitate any client activity that benefits such organisations.

2. Purpose of the Policy

This policy ensures that TC:

- Complies with UK counter-terrorism legislation
- Prevents financial or reputational risk
- Protects clients, staff, and the public
- Maintains ethical and lawful business operations
- Provides clear guidance on prohibited partnerships

- Establishes reporting duties for suspicious activity

3. Scope

This policy applies to:

- All business transactions
- Supplier relationships
- Donations, sponsorships, grants
- Partnerships and collaborations
- Procurement and contracting
- Client-funded activities
- Marketing, events, and community engagement

No part of TC's operations may involve or benefit any proscribed or extremist organisation.

4. Definitions

Radicalism

Ideas or actions that challenge democratic values, human rights, or lawful governance, often used as a pathway to extremist ideology.

Extremism

Vocal or active opposition to fundamental values such as democracy, rule of law, individual liberty, equality, and respect for different faiths and beliefs. Includes violent and non-violent extremism.

Terrorism

The use or threat of violence to influence political, religious, or ideological outcomes. *(Disclaimer: Terrorist organisations are responsible for severe harm, loss of life, and human rights violations.)*

Proscribed Organisation

An organisation formally banned under UK law or designated by international authorities due to involvement in terrorism or extremist activity.

5. Prohibited Activities

TC must not:

- Partner with
- Donate to

- Sponsor
- Promote
- Contract with
- Purchase from
- Provide services to

any organisation that:

- Is proscribed under UK law
- Is designated by international authorities
- Is known to support extremist or terrorist activity
- Has been judged by a competent court or authority to promote radicalism or extremism

Client-Funded Sponsorship Prohibition

Clients may not:

- Request donations to extremist-linked organisations
- Use companionship time or resources to support such organisations
- Ask staff to facilitate contact or engagement with such organisations

TC will decline any request that breaches this policy.

6. Existing Business Relationships

6.1 Pre-Existing Transactions

If TC is already transacting with an organisation **before** it becomes proscribed or designated:

TC will:

1. **Immediately suspend all new transactions**
2. Conduct an urgent compliance review
3. **Continue only essential existing transactions** *if and only if*:
    - The organisation has **formally appealed** the designation **AND**
    - A competent court has **granted a stay of execution**, injunction, or temporary relief permitting continued operations
4. Limit interactions strictly to essential, legally-permitted activities
5. Prepare for immediate termination if:

    - The appeal is dismissed
    - The stay is lifted
    - The court upholds the designation
    - Authorities instruct cessation
6. Document all decisions, legal advice, and communications

6.2 Appeal Process

During an appeal:

- No expansion or renewal of the relationship
- No discretionary or non-essential transactions
- Continuous monitoring of legal status
- Immediate termination once the appeal is resolved unfavourably

7. Due Diligence Requirements

TC will conduct:

- Annual screening of all suppliers and partners
- Pre-contract checks against UK and international proscription lists
- Ongoing monitoring for changes in status
- Enhanced due diligence for high-risk sectors

Concerns must be escalated to:

- Managing Director
- Compliance Lead
- Safeguarding Lead (if client safety is affected)

8. Whistleblowing & Reporting Duties (NEW SECTION)

8.1 Whistleblowing Principles

TC adopts international best-practice whistleblowing standards, ensuring:

- Protection for staff who report concerns
- Confidential handling of reports
- Non-retaliation
- Compliance with UK whistleblowing legislation
- Clear reporting pathways

8.2 Duty to Report Suspicious Activity

This policy **empowers and requires** all TC staff to **report (not investigate)** any suspicious activity or behaviour that may relate to:

- Radicalisation
- Extremism
- Terrorism
- Support for proscribed organisations
- Attempts to involve TC in prohibited activities

8.3 Reporting to Authorities

TC will report concerns to the appropriate governmental authority **in accordance with UK law**, including:

- Local Prevent Team
- Police
- Counter Terrorism Policing
- Home Office
- Relevant safeguarding authorities

8.4 Staff Must Not Investigate

Staff must:

- **Report immediately**
- **Not investigate**
- **Not confront individuals**
- **Not gather evidence**
- **Not make assumptions**

8.5 Protection for Whistleblowers

TC guarantees:

- No retaliation
- Confidential handling
- Support for staff raising concerns
- Compliance with the Public Interest Disclosure Act 1998

9. Record Keeping

TC will maintain:

- Due diligence records
- Screening results
- Risk assessments
- Termination decisions
- Appeal documentation
- Whistleblowing reports
- Communications with authorities

Records must be stored securely and in compliance with UK GDPR.

10. Staff Responsibilities

All staff must:

- Follow this policy
- Complete Prevent Duty training
- Report concerns immediately
- Maintain professional boundaries
- Avoid any personal involvement with extremist organisations

Non-compliance may result in disciplinary action.

11. Relevant Legislation

This policy aligns with:

- Terrorism Act 2000
- Counter-Terrorism and Security Act 2015
- Prevent Duty Guidance
- Public Interest Disclosure Act 1998
- Human Rights Act 1998
- Equality Act 2010
- Care Act 2014
- Data Protection Act 2018 / UK GDPR
- UN Security Council Sanctions Framework

12. Related Organisational Policies

- PRN-131 Prevent Duty Awareness Policy
- PRN-003 Adult Safeguarding Policy
- PRN-014 Code of Conduct
- PRN-099 Professional Boundaries Policy
- PRN-112 Data Protection & GDPR Policy
- PRN-102 Compliance Monitoring Policy
- PRN-063 Quality Audit & Inspection Procedure
- PRN-023 Confidential Information Management Policy

13. Policy Review

This policy will be reviewed:

- Annually
- After legislative changes
- After any incident involving extremist concerns
- At the request of the Managing Director or Compliance Lead