Operational Security and Terrorism Policy and Procedures

V1

November 2025

Policy Reference Sheet
Operational Security and Terrorism Policy

Document Properties	
Version	1
Author/Owner	Samar Chakraborty
Date of Issue	11/11/2025
Review Date	November 2026
Circulation	Public
Internal or External	External

Change Control			
Version Number	Page	Reason for changes made	Date

	Policy Component	Description	Check
1	Policy Statement	**This document is the British Horse Society's policy for Operational Security and Terrorism.** *The primary aim of this policy is to set out how the Society will respond to the potential terrorist threats it may face and provide procedures for employees (and other users) to follow in case a terrorism threat is realised.*	
2	Policy Audience	1. All employees, volunteers, contractors, BHS events and third-party vendors 2. BHS Home Team and One Team engaged in work activities off BHS premises. 3. All personnel responsible for managing, accessing, or securing physical and digital assets. 4. Operations across domestic and international activities by BHS assessors.	
3	Review Programme	Next review date is November 2026 Policy will be reviewed and approved by the Policy Review Group	

1.0 POLICY STATEMENT

British Horse Society (BHS) aims to raise awareness of potential security threats and terrorist related activities and minimise these wherever possible to provide a safe working environment for all of the Home Team and One Team. The purpose of this policy and associated procedures is not to be alarmist or cause undue fear or anxiety, but rather to be proactive, prepared and ensure employees understand their roles and responsibilities. The BHS strives to promote a culture which will help mitigate security risks by promoting compliance with security measures, awareness and vigilance.

The Society's Commitments:

1. To provide a safe environment for the Home Team and wider One Team using effective risk management policies.
2. Review of risk management controls.
3. Have robust policies, procedures and technology to prevent cyber attacks

4. Maintain robust operational security practices to promote a culture of vigilance and resilience
5. Ensure compliance with national security laws and other relevant laws to mitigate terrorism-related threats
6. Effective roll out and communication of any safety measures implemented.

Home Team and One Team Commitments:
Employers and premises owners must ensure the safety of staff and visitors, which includes preparing for emergencies such as terrorist incidents. They must also take reasonable care to avoid actions or omissions that could affect others in the workplace, in accordance with the BHS Health & Safety Policy, training requirements, and other available guidance.

BHS is required to assess threats—including terrorism—and identify vulnerabilities. These assessments inform the development of protective measures and emergency planning.

2.0 PROCEDURE

2.1 Identifying Vulnerabilities

BHS considers that its employees, volunteers, contractors, stakeholders, and visitors to BHS premises—including those working at external events (whether BHS, BRC, or non-BHS)—are at risk in the event of a physical attack. BHS further recognises that its physical assets, including all owned and leased premises, associated equipment, and vehicles in use, are also vulnerable to risk if not properly safeguarded.

BHS ensures that Martyn's Law 2025 is applied to its premises and events where applicable (see Appendix 6). BHS has a legal duty under this legislation and Counterterrorism and Security Act 2015 act, to be better prepared to respond to and mitigate the impact of a terrorist attack taking proportionate steps to safeguard people where needed.

To promote the safety and security of its people, premises, and assets, BHS ensures the following measures are in place.

For People:

- The People Team carry out a screening process as a part of recruitment policy.
- All prospective employees provide valid proof of identity (e.g., passport, driving licence, national insurance number).
- All employment offers are subject to the successful completion of right-to-work verification, criminal background checks (where applicable), employment history review, and references from previous employers. Please refer to paragraph 8 within the BHS Recruitment and Selection Policy for further guidance.
- Contractors, agency workers, and temporary staff vetted to the similar standard where applicable.
- Access to sensitive personnel records will be restricted to the People Team.
- A visitor sign-in system (Entry site) is in place, and no visitors are permitted to enter the office without identity verification to significantly reduces potential threats from unauthorised individuals within the building. Please see Appendix 5 for more information.
- A confidential reporting system is in place to ensure that employees are encouraged to report any suspicions that a colleague may be involved in, or is being indoctrinated into, a terrorist organisation. Please refer to the Whistleblowing Policy for further guidance.

For Premises:

- Letters, parcels and other deliveries received
    - from a trusted or known sources
    - deliveries are properly addressed to known person or department

- inspect deliveries and exercise caution when receiving or opening letters or parcels. Follow the information describe in appendix 3.
- use trusted suppliers wherever possible.
- recognise threat level and assess potential threats against the current national threat level, the impact and the likelihood of occurrence. See appendix 1 &2 for further information.

For Vehicles:

- Enhance vehicle security by implementing following measures:
  - The users of BHS vehicles need to act appropriately to secure BHS vehicles and protect employees and others to prevent using vehicles as a weapon as it has become a real threat in recent years.
  - BHS employees will be responsible for ensuring any vehicle used for BHS business is suitably secure & locked when unattended. This includes during loading and unloading and when taking breaks.
  - If possible, lock the doors of the vehicle when you are moving. This helps protect you from physical attack at times when you could be vulnerable such as in slow moving traffic or stationery at lights/junctions.
  - When loading or unloading the vehicle either on BHS property or other sites, remain vigilant for unauthorised personnel.
  - Never take unknown passengers in a BHS vehicle as this leaves equipment and vehicles open to theft and drivers open to risk of attack.
  - In the event of the theft of your vehicle or equipment, contact the police on 999 and notify your line manager.
  - If you are the victim of a theft, or you witness a theft from a BHS vehicle you MUST NOT try to approach or stop the thief or get into any altercation.
  - If you are threatened whilst in or around a BHS vehicle, DO NOT get into an altercation and try to leave the situation on foot or by using the vehicle if safe to do so. Contact the police on 999 and notify your line manager when safe to do so.

For Digital Assets:

- Aligns with the following compliance and legal framework to eliminate threat from digital assets
  - UK National Cyber Security Centre (NCSC) guidelines
  - GDPR and Data Protection Act 2018
  - Conduct regular digital security reviews by the IT department (please see appendix 7 for further information)

For Bomb Threat:

- Implement following measures when receive a bomb threat
  - Immediately notify the police by calling 999 and inform the Head of Operations, HSE Manager, Building Manager or someone from the Senior Management Team
  - Stay calm and listen to the caller
  - Obtain as much as information as possible - try to get the caller to be precise about the location and timing of the alleged bomb and try to establish whom they represent. If possible, keep the caller talking
  - Make a note of any number showing on the automatic number display on Microsoft Teams
  - If possible, make notes about what the caller sounds like (sex, age, any accent) any background noise (outdoor, vehicles, other people talking) and the exact wording they use.
  - Follow the safety measures described in appendix 8
  - Report the accident or incident to the Health and Safety Team, along with any supporting evidence, as soon as possible in accordance with Appendix 4.

3.0 Appendix:

Appendix 1:

Recognising Potential Threats

BHS employees and property could face a range of threats, both direct and indirect which can range in seriousness from low key to critical. The current threat level in the UK can be found on the MI5 website https://www.mi5.gov.uk/. Threat levels are classified as one of the following:

- LOW – means an attack is highly unlikely
- MODERATE – means an attack is possible, but not likely
- SUBSTANTIAL – means an attack is likely
- SEVERE – means an attack is highly likely
- CRITICAL – means an attack is highly likely in the near future

Appendix 2:

Direct Threats

- A member of a terrorist organisation could attempt to infiltrate the BHS by being recruited.
- Alternatively, a terrorist group may target an existing employee to indoctrinate them and recruit them into carrying out business for the group.
- The BHS Head Office, Stirling Office, externally run BHS/British Riding Clubs events and employees could be at risk from a physical attack by either a terrorist group or Lone attack
- The BHS run a small fleet of small and medium size vehicles. These have been commonly used in recent 'vehicles as weapons' attacks around the world.

Indirect Threats

- The presence of BHS at externally organised events not run by BHS carries an increased risk of disruption from activists targeting the event organisers.

Digital Threats

- IT Networks are always at risk from hackers or potential new viruses.

Appendix 3

Employees who open significant volumes of post should do so with letter openers and with minimum movement, hands are to be kept away from noses, and mouths, use mask and always wash hands after such work.
Employees should not blow into envelopes or shake them.
If a suspicious letter or package is received, the employee who discovers it—or someone nearby—should immediately evacuate the area, notify the police, and inform the Head of Operations, Building Manager, HSE Manager or a member of the Senior Management Team, who is immediately available.
Report the incident to the Health, Safety and Environment (HSE) Manager for further investigation and documentation.

Letter Bomb/Suspect Package Identification:

1. Delivered items can include letters, packets and parcels and may contain:

- explosive or incendiary devices
- sharps or blades
- offensive materials
- chemical, biological or radiological (CBR) materials or devices.

2. Delivered items come in a variety of shapes and sizes; a well-made one will look innocuous but there are many possible indicators that a delivered item may be of concern:

- a padded envelope ('Jiffy Bag') or other bulky packaging
- additional inner envelope or other contents that may be difficult to remove
- labelling or excessive sealing that encourages opening at a particular end or in a particular way
- oddly shaped or lopsided
- envelope flap stuck down completely (normally gummed envelope flaps leave slight gaps at edges)
- marked 'to be opened only by' 'personal' or 'confidential'
- unusual origin postmark and/or return address or no postmark/return address
- no return address or return address that cannot be verified
- poorly or inaccurately addressed or address printed unevenly or unusually
- more stamps than needed for size/weight of package
- greasy or oily stains emanating from within

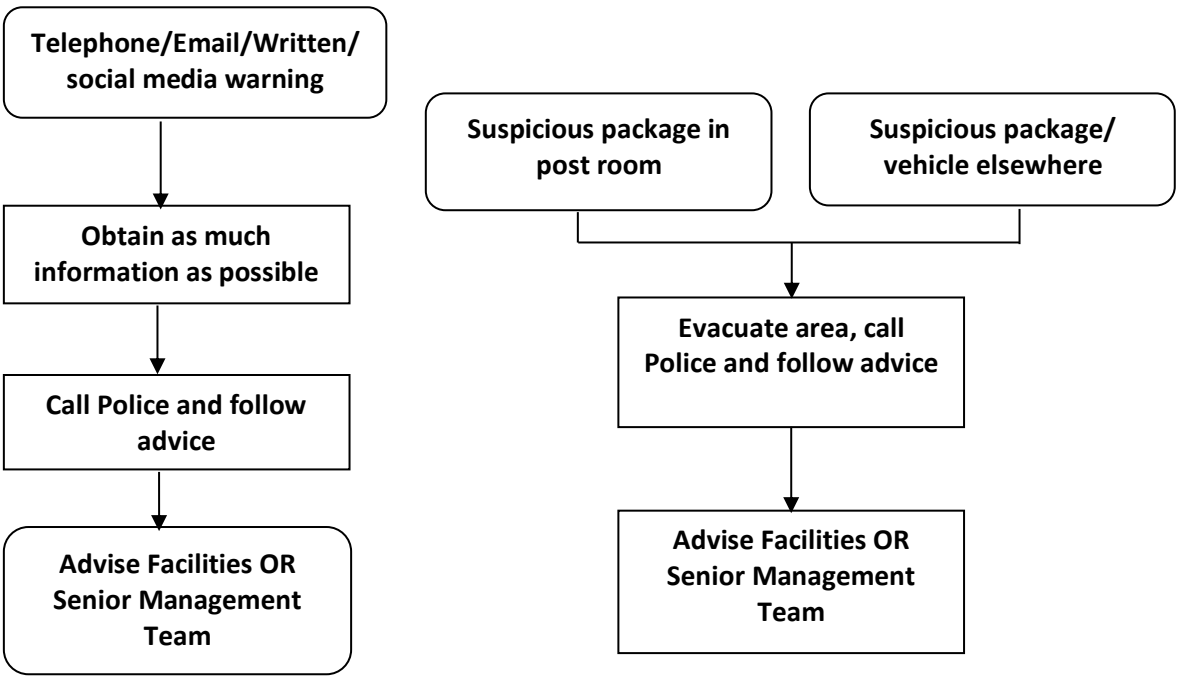
3. Additional explosive or incendiary indicators:

- unusually heavy or uneven weight distribution
- small hole(s) in envelope or wrapping

4. Additional CBR indicators:

- powders, liquids or odours emanating from package
- wrapping stained by liquid leakage
- unexpected items or materials found in package on opening (loose or in a container): powdered, crystalline or granular solids; liquids; sticky substances or residues
- unexpected odours observed on opening
- sudden onset of illness or irritation of skin, eyes or nose

Appendix 4:
Responding to an Incident – Incident Flowchart



Appendix 5:
Unauthorised Visitors

- If you see someone in the reception area of Head Office, do not give them access to the building until you have questioned who they are visiting and confirmed this with the employee.
- Reception at Head Office is a manned area. There is no manned reception area allowing direct access to the Stirling Office. All visitors should be arranged in advance wherever possible.
- If you have a visitor coming to Head Office they can enter through the main doors into the reception area of the building, use the screen to sign themselves in and this will then send an email to the BHS employee they are visiting to alert you your visitor is here. You meet with them and let them into the building.
- To improve building security at Head Office magnetic locks have been installed on the office entry doors to restrict access to authorised personnel only, using their allocated identity cards.
- The programming of 'Entry site' identity card is controlled by the Facilities Team.

Appendix 6:

Martyn's Law 2025 is set to take effect from April 2027, applies to a wide range of publicly accessible locations. If a BHS premises or event is open to the public and falls within either the Standard Duty Premises tier (200–799 capacity, including employees) or the Enhanced tier (800+ capacity, including employees), the following measures will apply.

Requirements for standard duty premises: applicable to events with 200–799 attendees.

- Appoint a designated responsible person who is accountable for implementing safety measures

- Notify the Security Industry Authority (SIA) of their premises; and have in place, so far as reasonably practicable in accordance with appropriate public protection procedures.

- Measure in place to reduce the risk of physical harm being caused to individuals relating to evacuation, invacuation (moving people to a safe place), locking down the premises, and communicating with individuals on the premises.

Requirements for enhanced duty premises and qualifying events: applicable to events with 800 or more attendees.

- The requirements set for standard duty premises must be maintained.

- A document is prepared and kept up to date, containing—
  I) public protection procedures and measures in place, or proposed to be put in place, and provide this document to the SIA.
  ii)an assessment and measures in place of how those procedures may be expected to reduce the risk and vulnerability.
  iii)The person must ensure that a copy of the document is provided to the Security Industry Authority—
  iv) as soon as is reasonably practicable after it is prepared, and
  v) if it is revised, before the end of the period of 30 days beginning with the day of its revision
  (ref. Martyn's Law Factsheet – Home Office in the media)

Appendix 7:

Digital assets at risk include:

- Data assets including Member and Donor information (names, addresses, history) Volunteer and colleague personal data, and financial records.
- IT infrastructure (servers, databases, email accounts, cloud storage, networks) software, and communication platforms.
- Website content and CMS, Social media accounts/content, marketing/brand materials, and usernames and passwords.

Appendix 8:

Safety Measures

In the rare event of an attack at Head Office, the Stirling Office or at external events employees are to
RUN, HIDE, TELL

1. RUN – to a place of safety. This is a far better option than to surrender or negotiate. If there's nowhere to go, then
2. HIDE – it's better to hide than to confront. Remember to turn your phone to silent and turn off any vibrate mode. Barricade yourself in if you can. Then finally and only when it is safe to do so
3. TELL – the police by calling 999

- If hiding whilst making a 999 call it may be dangerous to speak, in which case you should use the system called Silent Solutions which helps callers who cannot speak to an operator.
- A silent 999 call will not produce an emergency service response. To summon help you should do the following:
    1. Dial 999
    2. Listen to the operator's questions
    3. If possible, cough or make another noise to let the operator know you are there
    4. Then dial "55" on your keypad to summon help
    5. If no noise is made and 55 isn't keyed in, the call handler will assume it's an accidental call and hang up