Blue Light Whistle Blowers – Draft Risk Assessment and Mitigation in Preparation for the Launch

1. Operational & Data Security Risks

Breach of Confidentiality: This is the highest risk. If a whistleblower's identity is revealed, it could lead to detrimental treatment.

- *Mitigation:* Implement secure, encrypted IT systems for reporting; strict data access controls; and a clear, written whistleblowing policy.
- IP addresses should not be collected and voice calls should not be recorded.
- Those making disclosures have the opportunity to go on the record with their disclosure, in which case BLWB will ask for consent to disclose, or off the record, in which case no personal data is collected about the whistle blower and the information is shared with the relevant blue light service as an anonymous disclosure.
- In all cases a Data Sharing Agreement (DSA) will need to be put in place with the appropriate blue light service.

Improper Handling of Disclosures: Ineffective triage or investigation of reports can lead to missed wrongdoing.

- *Mitigation:* Develop clear, documented processes for report handling, ensuring confidentiality, and providing secure channels (e.g., encrypted emails).
- The purpose of BLWB is to quickly highlight wrong doing, a documented process is to be prepared in advance of the launch.

Data Protection (GDPR) Breaches: Handling sensitive personal data from whistleblowers.

- *Mitigation:* Robust, secure data storage and trained staff on confidentiality and data protection.
- BLWB must store the minimum amount of personal data, which should be held in an encrypted format on a cloud based main stream server provider such as AWS, Microsoft or Google.

System Vulnerability: A new charity may lack robust, audited systems.

- *Mitigation:* Use trusted, secure, third-party reporting platforms if possible.
- Work in conjunction with Protect and Crime Stoppers to replicate best practice.

2. Legal & Compliance Risks

- **Failure to Protect the Whistleblower:** Although PIDA (Public Interest Disclosure Act) protects workers, it does not explicitly cover volunteers, which often constitute a large part of a start-up charity.
    - *Mitigation:* Treat all reporters (workers and volunteers) as whistleblowers to build trust and ensure safety.

    - There is no reason to disclose names, if a reference number is given to each whistle blower.
    - However, a reference number will only work for verbal disclosure, individuals making an anonymous disclosure using the online form will not get a reference number unless IT can develop an onscreen solution.
- **Handling of False or Malicious Claims:** While rare, false information can be provided.
    - *Mitigation:* Legal review of policies to ensure they distinguish between, and appropriately handle, malicious allegations versus genuine, mistaken reports.
    - Where evidence indicates that the report is false, such as the complainant laughing and joking, this will be shared with the appropriate blue light service. However, as a basic principle we must treat reports as factual until the blue light service advises otherwise. BLWB provides a reporting service, it does not investigate allegations.
- **Regulatory Non-compliance:** Failure to comply with charity commission guidance.
    - *Mitigation:* Reviewing the Charity Commission's "Charity Sector Risk Assessment 2025" and ensuring policies align with legal requirements.
    - A review is underway to put in place the appropriate policies.

3. Reputational & Cultural Risks

- **Mistrust in Reporting Mechanisms:** Potential whistleblowers may not trust a new, unknown charity, making them hesitant to report.
    - *Mitigation:* Build a strong, transparent brand and clearly outline the confidentiality and protective measures in place.
    - Where possible BLWB will get buy in from the appropriate blue light service so that the reporting number and website can be shared in the work place via stickers, literature etc.
- **Victimisation of Whistleblowers:** The risk of reprisals against those who speak up.
    - *Mitigation:* A clear, zero-tolerance policy on retaliation, with staff training on how to support whistleblowers.
- **Perception of Bias:** If the charity is seen to be siding with either the whistleblower or the accused.
    - *Mitigation:* Establishing an independent, impartial investigation team or process.
    - All messages must be neutral and emphasis that BLWB is independent with its own Trustees who are not employed by any of the blue light services.

4. Financial & Governance Risks

- **Limited Financial Resources:** Start-ups like BLWB have limited cash flow.
    - *Mitigation:* Create a detailed, reviewed, and updated budget that aligns with operational costs.

    - Current funding will allow the charity to modestly operate for 12 months based on providing a helpline number, website and trustees and volunteers taking calls.

- **Poor Governance Structure:** A lack of clear, professional oversight, especially if it is volunteer-led.
    - *Mitigation:* Ensure a board with appropriate skills, clear conflict-of-interest policies, and regular, documented financial reviews.
    - Recruit further trustees with relevant experience, such as retired senior blue light employees to provide guidance and active support.
- **Funding Dependency:** Reliance on one or two sources of income.
    - *Mitigation:* Diversify fundraising and seek sustainable funding models early.
    - To continue to develop diverse funding, especially from the blue light services when they buy into the independent solution offered.

5. Key Mitigation Steps

- **Develop clear Policies:** These need to be clear, written policies outlining how the charity operates.
- **Appoint lead trustees:** key actions require a designated, senior person (e.g., a trustee) to oversee the process.
- **Work where practical with other charities:** Utilise where possible best practice from charities like Protect to develop new and improve existing processes.
- **Train trustees and volunteers:** Ensure anyone handling reports knows the legal, ethical, and practical requirements.

Operating BLWB involves some unique risks, as the charity is both a regulator-adjacent entity and a target for sensitive disclosures. Therefore, this risk assessment also focuses on protecting the organisation, trustees, volunteers and any future staff employed, and those who whistleblower to BLWB.

6. Strategic and Governance Risks

- **Conflict of Interest:** Given the proximity to legal and regulatory bodies, ensure trustees have no conflicting roles that could compromise the charity's independence.
- **Regulatory Compliance:** Failure to meet the Charity Commission's evolving standards for 2026, including the **Serious Incident Reporting** requirements, can lead to statutory inquiries.
- **Mission Creep:** BLWB must not get involved in anything that is outside the scope of reporting wrong doing, as this will bring the charity into conflict with the Charity Commission.

7. Operational and Data Risks

- **Breach of Confidentiality:** This is the most critical risk. Unauthorised disclosure of a whistleblower's identity can lead to severe legal and reputational damage.
- **Cybersecurity Threats:** Charities handling sensitive data are prime targets for hacking. Robust encryption and secure reporting channels are mandatory.
- **Information Veracity:** Acting on false or malicious reports can lead to litigation from the accused parties. Therefore, BLWB must make clear that it only provides a simple reporting service, it is down to the appropriate blue light service to determine whether the details provided are malicious and determining what actions to take is also down to the service.

8. Safeguarding and Wellbeing Risks

- **Staff Vicarious Trauma:** Employees, volunteers and trustees handling high-stress disclosures may suffer from mental health issues.
- **Action:** BLWB will need to develop a training programme and outsourced psychological support from a provider for around £15 per person per month.

9. Financial and Reputational Risks

- **Liability for Poor Advice:** If a whistleblower loses their job or faces legal action due to your guidance, the charity may be sued. Professional Indemnity Insurance is crucial.
- **Loss of Public Trust:** Scandals involving BLWB's own internal culture (e.g., "whistleblowing on the whistleblowing charity") can be fatal to fundraising and operations.
- **Action**: BLWB will need to take out Professional Indemnity Insurance.

Key Actions for 2026

1. Produce appropriate documents to support the charity, KC and JS to document and produce key items like a Safeguarding strategy.
2. GDPR compliance, PA to develop a data sharing agreement, and other mandatory items.
3. IT security, GP to develop a documented plan for keeping disclosures safe including some type of encrypted IT systems for reporting.
4. Review insurance DL and talk to Hiscox broker ref Professional Indemnity Insurance.
5. Develop a Risk Register, PA to use the Charity Commission's CC26 Framework to categorise and score risks by impact and likelihood.
6. Operational training, to ensure all volunteers, staff and trustees are trained – to be allocated.
7. Compliance training, PA including the Failure to Prevent Fraud offence and UK GDPR.
8. Financial, produce a simple budget for the next 12 months – to be allocated.