**Serious Incident Reporting Policy – Template & Guidance for Groups**

This document provides guidance and a template for IAM RoadSmart Affiliated Groups to develop their own Serious Incident Reporting Policy in line with good practice, legal expectations, and IAM RoadSmarts overarching standards.

**DISCLAIMER**
It is important to note that this guidance is for informational purposes only. It is the sole responsibility of each IAM RoadSmart affiliated Group to ensure their own policy is developed appropriately, kept up to date, and complies with any relevant laws or regulations. IAM RoadSmart is not responsible or liable for how affiliated Groups manage or respond to serious incidents.

**What is a Serious Incident?**

A serious incident is any event that results in or risks significant harm to:

* People (e.g. safeguarding incidents)
* Property or finances (e.g. theft or fraud)
* Reputation (e.g. inappropriate behaviour or negative publicity)
* Data and privacy (e.g. breach of personal data)

For IAM RoadSmart affiliated Groups, on-road incidents (such as serious collisions, injuries, or emergency service attendance during observed runs or assessments) are the most common type of serious incident and must be treated with the same seriousness and reporting standards as any other category.

Group examples include:

* Abuse, neglect, or harm to a member or volunteer
* Serious road accidents during assessments or Group events
* Financial loss due to fraud, theft, or mismanagement
* Criminal activity involving Group members or resources
* Data breaches involving sensitive personal information
* Legal claims against the Group

Please note that there is no definitive list of serious incidents, and Groups must apply judgement and seek external advice where necessary.

**Purpose**

Affiliated Groups must have clear procedures for identifying and responding to serious incidents that may occur during their activities. This supports:

* Compliance with UK charity law and the Charity Commission’s expectations.
* Protection of members, volunteers, and the public.
* Maintenance of public trust and group integrity.

**Scope**

This policy should apply to all:

* Group committee members
* Volunteers and Observers
* Members participating in Group activities
* Anyone else acting on behalf of the Group

**Reporting Responsibilities (Local Group Level)**

**Group Committees**

* Must ensure there is a named individual (e.g. Chair or Safeguarding Lead) responsible for handling serious incidents.
* Must investigate and take appropriate action.
* Must report qualifying incidents to the relevant bodies (e.g. Charity Commission, Police, ICO).

**Volunteers and Members**

* Must report any concerns or incidents immediately to a committee member or Group Chair/Safeguarding Officer.
* Can report anonymously if the Group has a whistleblowing mechanism.

**Reporting Procedure**

**Internal Group Process**
Each Group should:

1. Receive and log the incident using the Serious Incident Reporting Log, and where the incident involves an on-road event (e.g. collision, injury, emergency response), also complete the On-Road Incident Report Form located in the *'Observer documents'* section of the Group Management Dashboard.
2. Conduct a preliminary assessment to determine the severity and nature of the incident.
3. Take immediate action to safeguard individuals, assets, or data as needed.
4. Engage with relevant committee members (e.g. Chair, Safeguarding Lead) and/or your appropriate ASDM to agree on next steps and whether external reporting is required.
5. Document all decisions, completed forms, and follow-up actions in a secure and accessible location in line with data protection requirements.

**External Reporting**

If the incident meets the Charity Commission’s reporting criteria, the Group must:

* + Use the Commission's online form: [https://rsi.charitycommission.gov.uk](https://rsi.charitycommission.gov.uk/)
* Consider whether other authorities should be notified:
	+ **Police** – for criminal activity
	+ **ICO** – for data breaches
	+ **Local safeguarding boards** – for child or vulnerable adult concerns

**Confidentiality & Data Protection**

Groups must handle incident data in line with data protection law. Only individuals who need access to information should be involved. Personal data should be stored securely and retained only as long as necessary.

**Training and Awareness**

IAM RoadSmart Groups should:

* Provide regular briefings or training for committee members and volunteers on identifying and reporting serious incidents.
* Ensure new members and volunteers understand the policy.

**Consequences of Non-Compliance**

Failure to properly report and manage serious incidents may result in:

* Damage to the Group’s and IAM RoadSmart’s reputation.
* Regulatory scrutiny or penalties.
* Loss of public trust.
* Personal liability for Group committee members.