1. Risk Management Policy

2. Values Statement

RedR Australia ("RedR") is guided by its values of accountability, integrity, empathy, and collaboration. The Risk Management policy aims to provide protection for RedR personnel, assets, earnings and liabilities.

3. Purpose

The purpose of this policy is to identify the risks RedR Australia is exposed to, as well as determining the effectiveness of current mitigations measures.

4. Scope

This policy applies to:

- All employees, volunteers, contractors, and interns/work placements of RedR.
- Associate trainers.
- RedR deployees.
- Standby personnel/applicants.
- Board members.

5. Policy Statement and Principles

This policy seeks to embed good practice for risk management in relation to:

- Better identification and proactive management of opportunities and threats
- Improved incident management and reduction in loss and the cost of risk
- The development of a more risk-aware organisational culture through enhanced communication and reporting of risk
- A clear understanding by all staff of their roles, responsibilities, and authorities for managing risk
- More confident and rigorous decision making and planning from a corporate governance perspective
- Compliance with relevant legislation
- Stakeholder confidence and trust

Effective risk assessment can help ensure alignment with RedR Australia's organisational risk appetite and objectives. As such (prior to commencement) risk assessments should be conducted on any and all new:

- Contractual activities
- Partnership agreements
- RedR events (including training events)
- Associated fundraising and communications activities

Organisational approach to risk.
RedR Australia considers risk management a crucial prerequisite for the long-term viability of the organisation. The protection of personnel, earnings, assets, and liabilities against known and unknown losses in a cost-effective manner is a critical component of 'business as usual' (BAU) operations.

RedR Australia will adopt a planned and systematic approach to the management of risk. The requisite resources will be provided to enable successful implementation and continuous improvement of risk management processes in order to:

- Protect human life
- Minimise trauma
- Protect reputation (organisation, host agency and individual)
- Protect information
- Protect equipment and other physical assets

RedR Australia utilises a Risk Assessment Matrix approach to quantifying risk (see **Annex A**). This, in conjunction with robust context analyses and consideration of program criticality, is used to inform a holistic approach to risk management that draws upon best practice as described by ISO 31000:2018 (see **Annex B**). **Annex C** summarises the relationship between this document (the Risk Management Framework) and the processes of both risk management and risk identification.

Ensuring that an appreciation for risk management processes is present within all functional areas of the organisation is a core tenet of RedR Australia's approach to safety; risk management will be incorporated into the strategic and operational planning processes at all levels within RedR.

Partner organisations
RedR Australia will engage, consult, and involve partner organisations in the risk management strategy so they are aware of RedR risk policies and can assist in identifying and treating risks. Involving partner organisations will also assist them to gain information that informs their own risk management strategies.

Risk Identification Framework.
Incident classification plays a vital role in the effective monitoring and analysis of incident trends. **Annex D** summarises the way in which RedR Australia categorises risk. Risks (together with any incidents, or 'eventuated risks') are categorised by both type and sub-type.

Documentation Framework
The framework of operational risk management documentation is laid out in **Annex C**. These processes/documents are also referenced in the RedR Operations Manual.

It is important to note that considerations regarding security are integral to RedR in all of its work; therefore, many related policies related to Human Resources, Finance, Communications and Training all affect security. Contracts, both employment and for services, will also have an impact on security management.

6. Procedures

Risk management will be monitored using the RedR Australia Risk Assessment Criteria/Matrix on an ongoing basis and as a standing item of business at the Senior Leadership Team meeting.

The Chief Executive Officer's Board Reports will document and speak to Risk Management through an Exceptions Report which outlines risks and actions taken to treat them.

The Risk Register will be revised and updated by the Senior Leadership Team of RedR, the Audit and Risk Committee and the Board quarterly. The revision will address and identify risks in order of priority, identify strategies to treat risks, time frames, persons responsible and expected outcomes.

RedR Risk Management policy and associated assessment tools will be discussed, reviewed, and updated as a component of annual Board strategic review meetings. This information will be revised and included on the Strategic Plan.

Risks will be identified, reviewed, and monitored on an ongoing basis at nominated levels within RedR; this process will be led by the Head of Risk, Safety and Security. Further, stakeholders including staff will, through agreed consultative processes, be involved in assisting the Board to determine the acceptable level of risk (risk appetite) which will exist in relation to the activities of RedR under the identified categories.

The Chief Executive Officer (CEO), via the delegated authority of the Board, will ensure that RedR decisions and practices comply with the requirements of the relevant legislation, regulations and codes of conduct and practice. By extension, RedR managers will, with the support of the Head of Risk, Safety, and Security, ensure that staff within their teams understand their responsibilities with respect to operational risk, and will assist in fostering a risk aware culture and application of risk management tools.

Staff will make themselves aware of situations where someone or something may be at risk of harm or loss. They must then take reasonable action to assess the hazard/s, (see definitions) treat (eliminate, mitigate, transfer, accept, etc.) those hazard/s, evaluate the treatment, and escalate this information to the Risk, Safety, and Security (RSS) Team. The RSS team will then conduct a hazard inspection and add the hazard to the Risk Register as required.

Any risks falling in the 'Extreme' Residual Risk category *(see **Annex A**, page 10)* will be urgently brought to the attention of the Board via the CEO. Through the application of appropriate treatment actions, it is expected that the extreme risks reduce in significance. When these risks are reduced from the Extreme category, they will be taken off the Board agenda at that time.

This policy will be revised every two years by the Head of Risk, Safety, and Security, with modifications or amendments approved by the Board.

7. Roles and Responsibilities

The RedR Head of Risk, Safety and Security is responsible for ensuring the policy:

- Aligns with relevant legislation, government policy and/or RedR requirements/strategies/values,
- Is implemented and monitored, and
- Is reviewed to evaluate its continuing effectiveness.

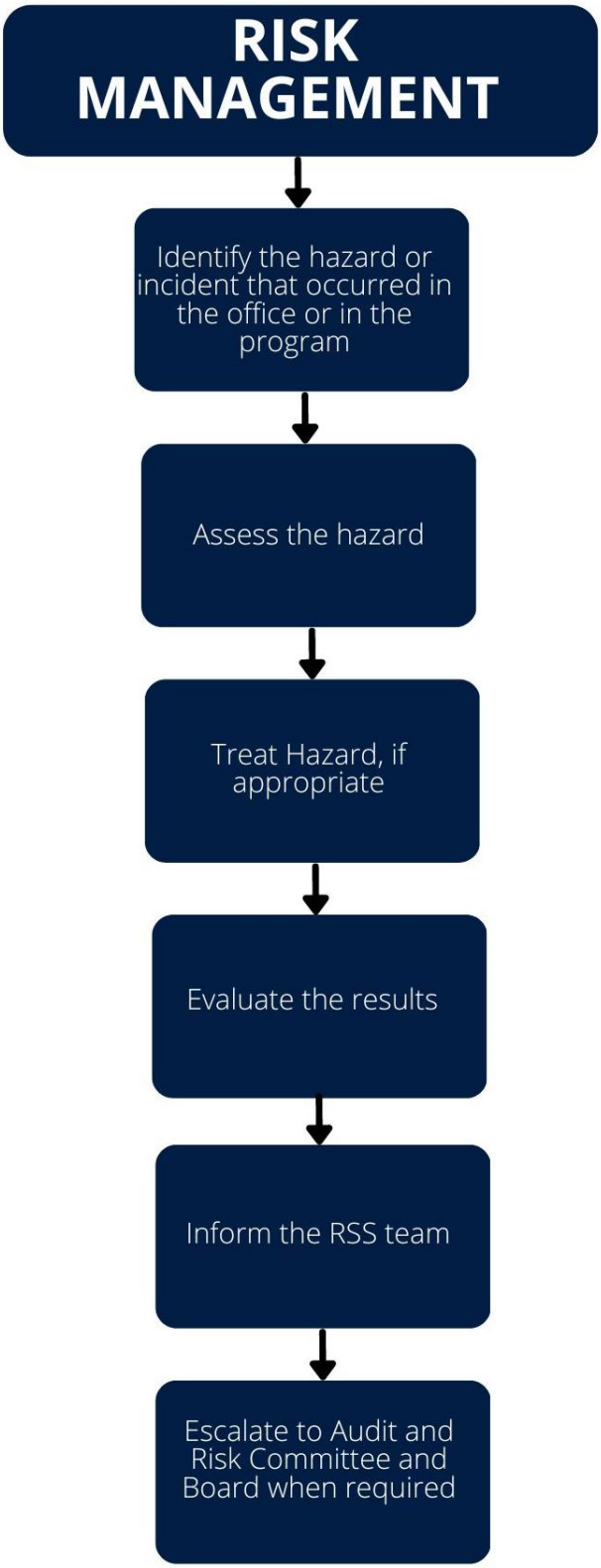
The CEO and Board Chair are responsible for ensuring the policy:

- Is implemented and monitored

The Audit and Risk Committee and Board members are responsible for:

- Ensuring the CEO and management team at RedR are meeting the boards legal obligations and expectations in managing risk.

8. Flow Chart


RISK MANAGEMENT
Identify the hazard or incident that occurred in the office or in the program
Assess the hazard
Treat Hazard, if appropriate
Evaluate the results
Inform the RSS team
Escalate to Audit and Risk Committee and Board when required

9. Definitions

Program criticality	The extent to which a program and/or set of activities is deemed necessary for the achievement of organisational objectives.
Reasonable action	That which is acceptable, fair, honest, proper and would be considered reasonable for a similar organisation to take, considering the nature and severity of the risk of harm or loss, knowledge of severity of harm or loss, knowledge of solutions, availability of solutions, legal requirements and cost of solutions
Risk	Effect of uncertainty on objectives [ISO 31000].
Risk appetite	The amount of risk that an entity is willing to accept or retain in order to achieve its objectives.
Risk Assessment	Overall process of risk identification, risk analysis and risk evaluation [ISO 31000].
Risk Criteria	A collective term for tools employed to quantify risk categories, severity, and consequence.
Risk factor	An element which can provide a source of risk [ISO 31000].
Risk Management	Coordinated activities to direct and control an organisation with regard to risk [ISO 31000].
Risk Treatment	Process to modify risk [ISO 31000].

10. Related Policies and Documents

- Child Safeguarding Policy
- Travel Policy
- Global Security Policy
- Incident Response Handbook
- Ethics (Whistle blower) Policy
- Anti-Bribery and Corruption Policy
- RedR Values and Code of Conduct
- ISO 31000:2018 *Risk management — Guidelines*

11. Document Control

Reviewed by:	Head of Risk, Safety and Security
Approved by:	CEO
Review date:	February 2024
Next review:	February 2026
Distribution:	External
Version number	3.0

Annex A: Risk Criteria/Matrix and Acceptability

Impact (Consequence) Rating. Indicates the impact of the risk on RedR operations.

	Severity	Operational	Medical/Wellbeing	Financial	Reputational	Other
1	Insignificant	No or very limited disruption to field/work day.	Very minor medical/wellbeing incident self-managed or attended to by medical specialist and/or First Aider.	Net impact of less than 1% of turnover (organisational) or self-funded (individual).	No significant direct reputational impact.	*Risk Descriptors are not presented in an attempt to capture an exhaustive list of events with the potential to impact the organisation.* *Rather they offer examples of what incidents of the respective severity may look like in four key areas of organisational risk (**Operational**, **Medical/Wellbeing**, **Financial**, and **Reputational**) in order to promote a shared/ consistent understanding of the magnitude of each level.* *Risk Owners are then able to apply this more specifically to their area of responsibility/ expertise.*
2	Minor	Field day(s) disrupted as a result of administrative and/or bureaucratic issues.	Medical/wellbeing incident requiring brief attention by medical/wellbeing specialist.	Net impact of 1-2% of turnover.	Potential for adverse reputational impact internally or within sector.	
3	Moderate	Mutliple field days disrupted as a result of minor to moderate administrative issues.	Medical/wellbeing incident requiring out-patient admission (e.g. insect-borne disease, compassionate repat).	Net impact of 3-5% of turnover.	Adverse reputational impact at state/national level.	
4	Major	Multiple field days disrupted as a result of a serious (e.g. missing staff, illegal detention, relocation/ evacuation from conflict/disaster) event.	Life-altering (non-life threatening medical/wellbeing incident or event.	Net impact of 6-20% of turnover.	Major adverse reputational impact at international level.	
5	Catastrophic	Proximate threat to organsational integrity. Forced suspension or cessation of operations, and/or loss of a substantial part of the organisation.	One or more fatalities. Kidnapping or abduction. Proximate threat to life/long-term wellbeing.	Net impact of greater than 20% of annual turnover, or any time RedR's financial obligations threaten to exceed its capacity to fulfil them.	Potential for irreparable/ unrecoverable reputational damage.	
-NM	Near Miss	Lessons can be learnt from causal factors when something almost goes wrong, not only when it does. The suffix 'NM' (e.g. 3NM) denotes a near miss; this signifies an incident where only a fortunate break in the chain of events leading up to the occurrence prevents harm from eventuating.				

Likelihood. Provides an assessment of the likelihood of the risk occurring.

Level	Scale	Description	Probability*
1	Rare	The event is likely to occur only in highly exceptional circumstances, there is no known occurrence. Extremely remote chance of occurrence in a financial year. 'Once in a lifetime' event.	< 2%
2	Unlikely	The event could occur at some time and has occurred sometime in the world. However, it would not be classed as a common occurrence and would only occur in certain remote circumstances.	2-16%
3	Probable	The event might occur at some time. Has occurred in Australia and the humanitarian/development industry in the past. Occurs either in RedR or the industry on a regular basis and frequently enough to be more than a remote possibility.	17-50%
4	Likely	The event will probably occur in most years and has occurred within RedR history. Knowledge or evidence either within RedR or within the humanitarian/development industry suggests this event occurs at regular intervals.	51-84%
5	Almost Certain	This event is expected to occur in most circumstances. Has occurred within RedR within the last year. The occurrence of this event is common and expected.	> 85%

Inherent/Residual Risk Levels (Risk Matrix). Risk levels are assessed by combining the impact of a given risk with the likelihood of it occurring. In this way the table below shows the risk grading of activities. The potential subjectivity of such quantification notwithstanding, using tables such as the below can be a useful means of identifying indicative levels of risk against which to contextualise the need to apply controls and/or reconsider activities.

		Impact (Consequence) Rating				
		(1) Insignificant	**(2) Minor**	**(3) Moderate**	**(4) Major**	**(5) Catastrophic**
Likelihood	**(5) Almost Certain**	(5) Moderate	(10) High	(15) Very High	(20) Extreme	(25) Extreme
	(4) Likely	(4) Moderate	(8) High	(12) Very High	(16) Very High	(20) Extreme
	(3) Probable	(3) Low	(6) Moderate	(9) High	(12) Very High	(15) Very High
	(2) Unlikely	(2) Low	(4) Moderate	(6) Moderate	(8) High	(10) High
	(1) Rare	(1) Low	(2) Low	(3) Low	(4) Moderate	(5) Moderate

Control Requirements, Risk Acceptability and Risk Appetite. The below table indicates a general expectation for corrective treatment measures required (i.e. controls) relative to inherent/residual risk. This table is indicative only. Regardless of the Risk Level, proportionate steps should be taken to always ensure the risk for each RedR activity is as low as reasonably practical.

Risk Level	Actions/Acceptability
Low	Activity can proceed.
Moderate	Activity can proceed. Logic demonstrating a correlation between primary threats/hazards and reasonable actions to treat them exists, and all reasonable steps have been taken to lower risk.
High	Activity can proceed only if there is a clear logic demonstrating a correlation between primary threats/hazards and reasonable actions to treat them and all reasonable steps have been taken to lower risk. Where this is the case, activity may proceed with the stated caveat that the risk is acceptable '*within the context of a fully (by UN or Other Host Agency) supported deployment to an environment acknowledged as being complex and potentially hostile*'.
Very High	Activity can generally not proceed until the risk level is lowered. SMT permission could be sought for specific/reasoned exemptions only where justified by exceptional circumstances/mission criticality.
Extreme	Activity cannot proceed until the risk level is lowered.

Annex B: Compliance notes on Risk Management Frameworks

There are many different risk management frameworks available to the risk manager. In Australia, AS/NZS/ISO 31000:2018 *Risk management — Guidelines* (referred to herein as simply 'ISO 31000') is the Australian Standard risk management framework. ISO 31000 requires consideration of the following:

1. Leadership and commitment to risk management
2. Integrating risk management across all aspects of the organisation
3. Designing a process for managing risk
4. Implementing a Risk Management Process
5. Evaluating the process
6. Continual improvement of the process

CONSIDERATIONS FOR MANAGING RISK

The risk management process provided by ISO 31000 outlines the following considerations:

- **Leadership and commitment.** Top management and oversight bodies, where applicable, should ensure that risk management is integrated into all organisational activities and should demonstrate leadership and commitment.
- **Articulating risk management commitment.** Top management and oversight bodies, where applicable, should demonstrate and articulate their continual commitment to risk management through a policy, a statement or other forms that clearly convey an organisation's objectives, assigns roles/authorities/responsibilities, and commitment to risk management.
- **Context.** Evaluating and understanding operational context.
- **Risk management policy**. Establishing policy that states risk management objectives and commitments.
- **Accountability**. Ensuring that those responsible for management of risk are appropriately competent, accountable and have the appropriate authority.
- **Integrated processes**. Risk management processes are integrated and embedded into organisational practices and processes, so they are not separate from other practices and processes.
- **Resourcing**. Adequate resources are allocated to risk management.
- **Internal reporting and communication mechanisms.** Accountability and ownership of risk is supported and encouraged by establishing internal reporting and communication.
- **External reporting and communication mechanisms**. Appropriate mechanisms are planned and implemented to communicate effectively with external stakeholders, including cases where there are legal or regulatory requirements.

RISK MANAGEMENT PROCESS

Risk management processes involve systematic application of management policies, procedures and practices to the task of identifying, analysing, evaluating, treating and monitoring risk. While various models may achieve this goal, a Risk Management Process should incorporate the following steps:

- **Establish the context.** What is the purpose, who is involved, in what threat environment are they operating, what oversight is required and what equipment may be needed?
- **Identify all hazards and risks.** What could potentially cause harm or loss?
- **Assess the risks.** Assess and prioritise risks and address in priority order. What could happen and what might be the consequences?

- **Evaluate risks and control measures.** Assess and choose measures to control the risks. Can you eliminate, avoid, reduce or manage the risk?
- **Treatment of risks.** Implementing the appropriate control measures to manage the risks.
- **Monitor and review.** An ongoing process needs to monitor and review the risk and control measures. Are the measures working, does the process meet relevant standards, what needs amending and/or are the activity goals or outcomes still being achieved?

Throughout the steps **communication between all relevant stakeholders should occur.** This enables important information to be shared and integrated into the Risk Management Process.

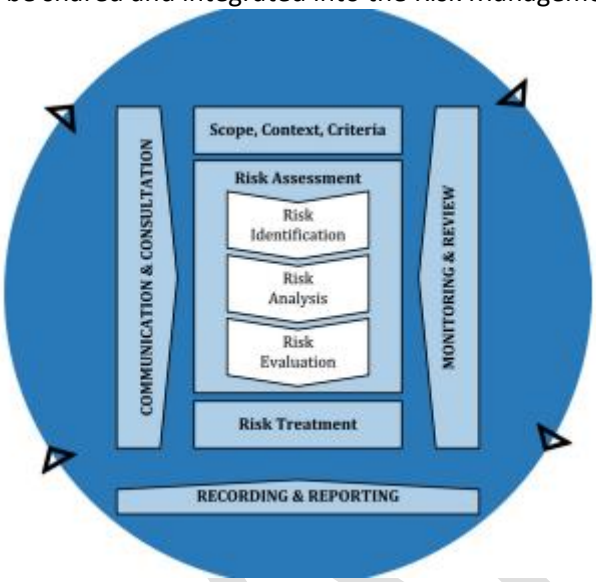


Fig.D1: Risk Management Process (ISO 31000:2018)

RISK IDENTIFICATION FRAMEWORK

Utilising specific, organisationally-appropriate risk categorisation can assist in the structured identification and management of risk. Consideration should be given to each of these risk categories in relation to the specific activities being undertaken and the type of participants involved. This consideration of participants should extend to specific understandings of risk as heightened/mitigated relative to individual capabilities and experience.

HIERACHARCHY OF RISK TREATMENT

Control measures have various degrees of effectiveness. Hazards and risks should be eliminated, where that is not possible, a hierarchy of control measures is employed. See below.

Eliminate hazards and risks	Highest level of protection and most effective control. Eliminating the hazard and the risk it creates is the most effective control measure.
Reduce the risk	Reducing risks with one or more of the following controls: Substitution (substituting risks with lesser risks); Isolation (isolating people from the risks); Engineering (reducing risks through engineering changes or changes to systems of work).
Administrative controls	Using administrative actions to minimise exposure to hazards and to reduce the level of harm. Administrative controls generally offer low levels of protection and are less reliable.

Personal Protective Equipment (PPE)	Using personal protective equipment to protect people from harm. Using PPE is the lowest level of protection and is considered the least reliable control.

RISK MANAGEMENT PLAN

By using the Risk Management Process and Risk Identification Framework, a 'Risk Management Plan' that identifies and treats risks can be completed. This is a key output from the Risk Management Process.

When developing and/or reviewing Risk Management Plans, consideration should be given to previous incidents and risk assessment outcomes that may include (and is not limited to):

- What has occurred within the organisation?
- What is public knowledge (e.g. inquests) based on similar organisations' experiences?
- What is public knowledge based on the type of organisational activity being undertaken?
- What is public knowledge based on similar types of organisational activities to that being undertaken (e.g. remote work undertaken by the development, security or even leisure sectors)?

RISK MANAGEMENT IMPLEMENTATION

Risk management is not something that stops after completing a Risk Management Framework and Plan. The Risk Management Plan actions need to be implemented and continually reviewed and adjusted. Any such review and adjustment during an activity is captured under the Dynamic Risk Assessment Process.

Annex C: Risk Identification Framework

Category	Type	Sub-type	Description
A	Overseas	Medical Illness Medical Injury Dental Loss/Theft Behavioural Corruption/Bribery Equipment Espionage Safeguarding Security (including civil unrest, terrorism and armed conflict) Sexual Exploitation/Abuse/Harassment Transport/Logistics Wellbeing/Compassionate Natural Disasters Mental Health and Psychosocial Support Road Traffic Accidents Sanctions	Any **overseas** risk event with the potential to impact the health or wellbeing of deployees/staff and/or directly impact service delivery. *Incidents of sanction violations and Sexual Exploitation and Harassment may need to be communicated to donor bodies/agencies, in line with the terms of the funding agreement.*
B	Financial	Compliance	Cash flow, change of government, insurance, fraud. *Incidents of alleged/suspected fraud may need to be communicated to donor bodies/agencies, in line with the terms of the funding agreement.*
C	Training	Trg. Medical Illness Trg. Medical Injury Trg. Equipment Trg. Wellbeing	Risk events associated with training and other contracted work.
D	Human Resources	Disciplinary/Grievance Equal Opportunities OH&S Recruitment Staff Wellbeing	Staff turnover, employment risk events, cohesion between Board and staff, staff leave, volunteer and associate trainer management, succession planning, WHS/OHS, compliance with relevant legislations, ISOs and codes.
E	Organisational/ Governance	Reputation Communications IP IT & Systems	Board and governance, IT, data loss/corruption intellectual property rights, privacy.
F	Strategic Partnerships	3rd Party	Risk events associated with external relations and organisational reputation including events management and fundraising, relations with program partners and donors.
G	Other	Facilities	Physical access to buildings. Other risk events not captured by the above.

Annex D: Operational Risk Management Documentation Framework

Governance Level	Direction from Board			
Strategic Level	1. Risk Management Policy			
	1.1. Risk Register			
	1.2. Incident Log – House on the Hill			
Policy Level	**PREPARATION** 2. Global Safety and Security Policy	**PREPARATION** 3. Training Course Risk Management Policy	**RESPONSE/RECOVERY** 4. **Incident Response Handbook**	**REPORTING** 5. Incident Reporting Policy
Implementation/Documentation	2.1 Country Notes	3.1. Course-Specific Risk Assessments	4.1. Standard Operating Procedures	5.1. Incident Reporting Form A
	2.2 Field Mission Travel Request	3.2. Site-Specific Risk Assessments	4.2. GAP Guardian	
	2.3 RedR Higher Threat SRA Template			
	2.5 Overseas Driving Policy/Request Form 2.6 Deployment Due Diligence Assessments 2.7 Host Organisation Due Diligence Assessments 2.8 HEAT Recognition of Prior Learning and Experience Decision Matrix 2.9 Office Security and Contingency Plans	**Related policies:** • MEAL Framework • HR (including Code of Conduct, Staff Travel Policy) • Finance and Administration (including IT) • Business Continuity Plan • OH&S • Communications (including Social Media) • Relevant national and international standards		