General Optical Council

GOC Never Events Framework

1. Introduction

1.1 The General Optical Council (GOC) defines a Never Event as an incident of the utmost criticality, which GOC internal controls should prevent from happening. Never Events require enhanced investigation and reporting using the incident review template (annex three).

1.2 The GOC recognises the importance of effectively managing its risks and learning from incidents. An important element in ensuring objectives are met is promoting a culture in which Never Events are reported at the earliest opportunity. Timely notification of incidents provides the organisation with an opportunity to address contributory factors and prevent a recurrence.

1.3 Developing a culture where staff feel confident to report incidents will contribute to and uphold GOC values. The Chief Executive and Senior Management Team (SMT) are committed to encouraging open and fair reporting and reporting of incidents. All staff can be confident that this approach will be adhered to at all times except where malicious, criminal, gross or repeated misconduct is involved.

1.4 The purpose of this document is to explain how the GOC will respond when they occur.

2. GOC Never Events

2.1 The GOC has described five Never Events. They are:

1) No registrant whether student or fully qualified individual or body corporate without the correct qualifications / identity or other documentary evidence, or fitness to practise suitability will be registered or restored to the register.

2) No registrant whether student or fully qualified individual or body a corporate will be suspended or removed from the register without approval and appropriate double checking by an appropriate manager.

3) No registrant whether student or fully qualified individual or body corporate who is non-compliant with our requirements relating to renewal or CET/CPD requirements to remain on the register (past expiry date);

4) No Fitness to Practise Committee order (substantive or interim) should lapse; expire; or fail to be reviewed without an authorised decision being

made that it is no longer necessary and/or that a review is not required; and

5) All registration status changes following a substantive or interim hearing, to be updated within three working days of the hearing concluding.

2.2 The Never Events list will be reviewed by the Director of Resources/Corporate Services (DoR) (with input from key staff) and the SMT on a regular basis to ensure that the incidents continue to reflect the definition of a Never Event and that prevention and control measures are up to date, adequate and are operating effectively. This also provides the opportunity for new Never Events to be added, as and when appropriate.

2.3 The types of incidents defined as Never Events have been identified using the following criteria:

a. Significant / serious patient safety implications

b. High level of reputational risk

c. Scored 5 on the risk impact scale (annex one)

3. Responsibilities

3.1 SMT will determine which incidents are included on the list of Never Events.

3.2 To ensure that there is a robust control environment supporting the management of the risks to which Never Events relate, the DoR is responsible for working with relevant Heads of Function on the effective design and operation of mitigating actions.

3.3 Heads of Functions are responsible for ensuring that there are documented processes/procedures which describe how tasks are to be undertaken so that Never Events do not occur.

What to do if a Never Event occurs

3.4 The person who identifies that a Never Event has occurred is responsible for immediately reporting the incident to their Head of Function or Director, and to the DoR, who will notify the SMT group without delay. For the purposes of reporting, suspected Never Events must be clearly identified as such, even if the status is uncertain at the time of report.

3.5 Due to the risk implications associated with Never Events, the director with responsibility for the area in which the incident occurred will assume the role of the risk owner. In the event the incident relates to areas in which more than one director has responsibility, the risk owner responsibility will be shared.

3.6 The DoR will agree with the relevant director(s) on who will investigate and report on the Never Event.

4. Investigations

4.1 It is important that if a Never Event occurs the problems in the case are identified and analysed through full investigation using a systems-based investigation method (see root cause analysis guidance – annex two) to understand how and why they occurred (from a systems perspective). This will mean effective and targeted action can be taken to prevent recurrence.

4.2 The incident reporting template (annex three) may be used as a starting point for communicating the result of the investigation. However, the investigation final report for a Never Event likely will require considerable detail and the Investigating Officer should determine the most effective format for presenting their findings and recommendations.

4.3 The DoR will assist the Investigating Officer ensure consistency in reports.

5. Reporting

Routine Reporting

5.1 All routine reporting related to Never Events is the responsibility of the Head of Secretariat, with support from the DoR.

5.2 Quarterly reports will be prepared for SMT on Never Events (by way of inclusion in the Significant Incidents Report). These will both support the operation of effective risk mitigation by providing control assurance and reinforce learning of lessons through progress updates on agreed actions from any previous Never Event.

5.3 As part of end-of-year reporting, a summary of Never Events investigations and key learning will be provided to Audit and Risk Committee.

Never Event Investigation Reports

5.4 Due to the serious nature of Never Events, it is important that they are responded to promptly. A draft report, agreed by the risk owner(s), should be circulated to SMT within 14 days of the incident being reported. SMT should sign off the final report within 28 days of the incident being reported.

Failure to report a Never Event

5.5 This framework is designed to provide staff with clarity on their responsibilities and what to do if a Never Event happens. It is important that we all work in a culture where openness, transparency and learning from the incident are key.

5.6 <u>A failure to report a Never Event is unacceptable</u> and can signal regulatory, cultural and safety failings in an organisation. In some circumstances, it may not be apparent that an incident is a Never Event until there has been some degree of investigation. In these circumstances, the possibility that a Never Event has occurred should still be reported as soon as it is identified.

5.7 Failure to report a Never Event should be thoroughly investigated by the Governance team, with support from the DoR, to understand what prevented the recognition and/or reporting of the incident. This may lead to efforts to develop knowledge/awareness about incident reporting and Never Events more specifically. It may also lead to broader initiatives to measure and improve reporting culture as part of a wider culture in the organisation. <u>If the failure to report was a deliberate act, this is likely to constitute a serious failing by the staff members involved under the Disciplinary Policy</u>, which refers to “Failure to follow GOC policy/procedure resulting in significant disruption or effect to the GOC”.

Annex one– risk impact scale

Impact					
DESCRIPTOR	1 INSIGNIFICANT	2 MINOR	3 MODERATE	4 MAJOR	5 CATASTROPHIC
Financial (damage/loss)	Organisational / financial loss (£< 1k).	Organisational / financial loss (£1,000-£10,000).	Organisational / financial loss (£10,000 - 100,000).	Organisational / financial loss (£100,000 - £1m).	Organisational / financial loss (£>1m).
Reputation & publicity	Limited negative local public exposure with negligible impact on stakeholder confidence.	Negative local public exposure with low impact on stakeholder confidence. Local media coverage <1day.	Negative local and limited national public exposure with moderate impact on stakeholder confidence and PSA	Negative national public exposure with significant impact on stakeholder confidence. Loss of public confidence.	Full public inquiry. MP concerns/ questions in parliament. Severe loss of confidence in the organisation.
Information Governance	**Potential** breach of confidentiality risk assessed as low, e.g. files/data was encrypted.	Serious **potential** breach of confidentiality e.g. unencrypted records/data lost.	Serious breach of confidentiality from inadequately protected PC(s), laptop(s) and remote device(s).	Serious breach of confidentiality with particularly sensitivity data.	Serious breach of confidentiality with potential for ID theft.
Information Technology	An event which leads to loss of critical business processes but can be managed under normal circumstances and resolved quickly and easily.	An event which leads to loss of critical business processes but can be managed under normal circumstances and resolved in around 1 day.	A significant event, which leads to loss of critical business processes but can be managed under normal circumstances and resolved in 1 or 2 days.	A critical event, which leads to loss of critical business processes, but can be resolved with proper management within a few days.	An extreme event, which leads to loss of critical business processes which takes significant management time and resources to resolve.

Legislative	Minor internal breach.	Significant internal breach.	Reportable incident to regulator, no follow up.	Report of breach to regulator with immediate correction to be implemented.	Report to regulator, prosecution or fines requiring major corrective action.

Impact					
DESCRIPTOR	**1 INSIGNIFICANT**	**2 MINOR**	**3 MODERATE**	**4 MAJOR**	**5 CATASTROPHIC**
Security	Very minor incidents/ damage to assets, property or personnel.	Localised incidents/ damage to assets, property or personnel with no effect on service delivery.	Organisational wide incidents/ damage to assets, property or personnel with some effect on service delivery.	Organisation wide incidents/ damage to assets, property or personnel with significant impact on service delivery.	Extreme incident with major effects on the organisation's ability to deliver core services.
Health & Safety	On-site exposure immediately contained. Trivial injury	On-site exposure, contained after prolonged effect. Minor injury	On-site exposure, contained with outside assistance. Major injury.	Prolonged/Major incident with serious casualties. Major injuries.	Major incident with fatalities.
Staffing and Competence	Short term low staffing level temporarily reduces service quality (< 1 day).	Ongoing low staffing level reduces service quality. **Minor error** due to ineffective training.	Late delivery of key objectives/service due to lack of staff. **Moderate error** due to ineffective training.	Uncertain delivery of key objectives / service due to lack of staff. **Major error** due to ineffective training.	Non-delivery of key objectives / service due to lack of staff. Loss of key staff **Critical error** due to ineffective training, systems, or process design.
Projects	Minimal impact on project.	Delay/ minor issues with project, but within tolerance.	Delay or issues with project outside of tolerances.	Uncertain delivery of project.	Non-delivery of project.

Annex two – Root Cause Analysis Guidance (The 5 Steps)

1. Gather as much data as possible – this will yield causes and supporting evidence
2. Data can be time sensitive – gather it as soon as possible after the incident
3. Not all evidence is equal – high-quality evidence tends to be objective (documents, emails, computer logs) – the more subjective the evidence is (personal recollections, uncorroborated statements, etc) the lower its quality and less it should be relied upon
4. All data/evidence collected must be stored securely so that it is not tampered with, destroyed or damaged
5. Good data storage should enable easy access for those who need it
6. Remember – there may be legal reasons for retaining evidence!
7. The Problem Statement describes clearly the gap between what happened and what should have been achieved. It should include:

   - the Focal Point (a one sentence description of the problem being investigated) / the date and time of incident / where the incident happened, and the system and process involved / what was the actual impact of the incident / what could the potential impact have been

8. A high quality Problem Statement contains a good level of detail and does not stray into mentioning any solutions (those come later!)
9. Root Cause Analysis uses a Causes & Effect chart to visually present causes and their logical relationships - this helps demonstrate the interaction of causes, effects and evidence, and help find solutions
10. There is no set methodology in RCA for ascertaining cause and effect, though a common technique is to use the ‘5 Whys’ (repeatedly asking the question “why” until reaching a point where all of the issues are fully understood)
11. It is perfectly acceptable to have more than one root cause!
12. There will likely be a number of options available to address the identified root cause(s) - in considering which to recommend, think about the effectiveness, ease of implementation, cost/benefit, and any potential negative consequences of the possible solutions
13. Recommendations should address all root causes identified by the process and concentrate specifically on eliminating or reducing the likelihood of recurrence
14. Solutions should be SMART – Specific, Measurable, Achievable, Realistic and
15. Clearly show how the proposed solution will eliminate the problem, and why this is the best course of action for the organisation to follow
16. Ensure there is a plan to monitor the implementation of the solution and the effect it is having – *without checking, how can the organisation be confident it has fixed the problem?*

Annex three – Incident review (read Root Cause Analysis Guidance first)

NOTE: This form has been designed to include future use as part of a wider incident management approach (not just for Never Events).

Click here to enter text.

Incident number (to be provided by Secretariat team): Click here to enter text.

Related risks: Click here to enter text.

Incident Impact: Choose an item.

Incident Category: Choose an item.

Introduction

Click here to enter text.

Findings from the incident review

Click here to enter text.

The issues

Click here to enter text.

Recommendations

1. Click here to enter text.

Actions

Action	Due date	By	Date completed
1.	**Click here to enter a date.**		**Click here to enter a date.**
2.	**Click here to enter a date.**		**Click here to enter a date.**
3.	**Click here to enter a date.**		**Click here to enter a date.**
4.	**Click here to enter a date.**		**Click here to enter a date.**

5.	**Click here to enter a date.**		**Click here to enter a date.**

Click here to enter text.

Click here to enter a date.