Checklist for implementing the CIISA Standards

Introduction

Organisations, productions or projects can assess their existing policies and procedures against, or create new ones aligned with, the CIISA Standards to ensure that they are embedding the right behaviours, and that their workforce know what is expected of them. Through consistently meeting the Standards, organisations, productions and projects will ensure they are promoting the behaviours and culture within their organisation, production or project that enable their workforce to thrive.

This document provides:

- A high-level checklist for implementing the CIISA Standards
- Examples of what to consider when completing the checklist

Checklist for implementing the CIISA Standards

When answering each of the questions below, organisations, productions and projects should also ensure that they have engaged stakeholders.

1. Stakeholder mapping: Who are the different people potentially affected by breaches of the CIISA Standards that you might need to consider?	
2. Policy: Do you have a code of conduct or policy/policies that reflect(s) the CIISA Standards?	
3. Risks: What situations present particular risks of breaches of the CIISA Standards?	
4. Actions: What actions have been put in place to prevent, mitigate or address breaches of the CIISA Standards?	
5. Tracking & monitoring: How is the effectiveness of the actions you are taking being monitored?	
6. Communications: How are commitments, policies, risks, progress and effectiveness communicated to stakeholders?	
7. Reporting mechanisms: What channels and processes are in place for receiving and handling concerns raised or reports of breaches related to the CIISA Standards?	
8. Reporting mechanisms - Confidentiality: Are confidential and anonymous options for reporting in place?	
9. Reporting mechanisms - Effectiveness: What checks are in place to ensure the reporting mechanisms are known about, accessible and trusted?	
10. Learning culture: How does your entity foster a culture that encourages feedback, how does it learn from issues raised and how does it demonstrate continuous improvement?	

What to consider when completing the checklist

For examples of what to consider for these questions and ways to ensure stakeholders are engaged throughout, see below.

Checklist questions	Examples	Stakeholder engagement
1. Who are the different people potentially affected by breaches of the CIISA Standards that you might need to consider?	Own staff, freelance workers, ancillary workers (cleaners etc), junior staff, people providing particular services, specific roles, members of the public, visiting artists, young/child artists, fans, people with certain characteristics	Who else can you ask to ensure your list is complete?
2. Do you have a code of conduct or policy/policies that reflect(s) the CIISA Standards?	Employee code of conduct; business principles; Supplier code of conduct; human resources policies	Who has been engaged in developing the code of conduct / policy?
3. What situations present particular risks of breaches of the CIISA Standards?	Types of event; specific countries; stages in a process; presence of children/young people; particular content or genres; financial arrangements; time of day	Who has been engaged to understand the nature of risks?
4. What actions have been put in place to prevent, mitigate or address breaches of the CIISA Standards?	Training; protocols; capacity building; recruitment practices; pay gap reviews; awareness-raising; mental health support; specialist advice; dedicated roles	Who has been engaged to ensure that actions are appropriate and likely to work?
5. How is the effectiveness of the actions you are taking being monitored?	Surveys; focus groups; formal/informal feedback; concerns raised; data tracking such as employee turnover, sickness rates, pay gaps, diversity stats, injuries, use of support offered	How is stakeholder engagement used to help track effectiveness?
6. How are commitments, risks, progress and effectiveness communicated to stakeholders?	Website; intranet; posters; call sheets; emails; briefings; peer champions; training sessions; workshops; townhalls; meeting cascades	Who is communicated with (and who might be missed out)?

Continues overleaf

Checklist questions	Examples	Stakeholder engagement
7. What channels and processes are in place for receiving and handling concerns raised or reports of breaches related to the CIISA Standards?	Helpline; designated staff to approach; survey; physical suggestion/feedback box; email inbox; regular meetings asking for feedback; written procedure on steps to take when complaint/issue raised (from triage to investigation to resolution); scenario-planning; tabletop exercises; non-retaliation policy	Which stakeholders fed into the development of channels and processes?
8. Are confidential and anonymous options for reporting in place?	Third party provider of speak up system; apps protecting confidentiality or anonymity	
9. What checks are in place to ensure the reporting mechanisms are known about, accessible and trusted?	Surveys; formal/informal check-ins with stakeholder; audits; independent monitoring	Who has been asked about the mechanisms' effectiveness?
10. How does your entity foster a culture that encourages feedback, how does it learn from issues raised and how does it demonstrate continuous improvement?	Mechanisms for gathering and responding to feedback; root cause analysis of issues and incidents; trend analysis to identify areas to address; commitment to review approach regularly; communications to share learnings and improvements	How are stakeholder views regularly sought and how do they feed into decision-making?