

Speaking up: Reporting concerns to CIISA

Guide for Organisations

What you can report, how we will handle it and what happens next

CIISA is not an emergency service. Call 999 if someone is in immediate danger or needs emergency medical help. Follow your own safeguarding and emergency procedures without waiting for CIISA.

This guide explains what organisations can report to CIISA, how to report and what happens afterwards. It also explains how we handle information and what CIISA can and cannot do.

About CIISA

We are an independent standards body for the UK's creative industries. Through [the CIISA Standards](#), we set clear and consistent expectations for behaviour in creative industry workplaces and help individuals and organisations put the CIISA Standards into practice.

CIISA is also a 'prescribed person' under whistleblowing law in Great Britain. Northern Ireland has separate whistleblowing legislation and its own process for appointing Prescribed Persons.

This means workers in film, TV, music and theatre can report certain concerns about wrongdoing at work to us where that is relevant to the CIISA Standards.

Whistleblowing means speaking up about wrongdoing at work that could affect others or raise wider concerns about the workplace.

Organisations can also share relevant concerns, findings and intelligence with us. **This is separate from whistleblowing** by an individual, but it equally helps us understand what is happening across the creative industries.

CIISA is not a statutory regulator. Being a prescribed person does not give us powers to compel people to give us information, to determine whether laws have been broken, impose sanctions or provide a remedy in an individual case.

We provide an independent and confidential place for people and organisations to report. We use their information to identify issues, themes and patterns and recommend improvements across the creative industries.

If you are an individual and want to report a whistleblowing concern to CIISA, please refer to our **guide for individuals**.

1. Thinking about reporting?

Why should my organisation report to CIISA?

CIISA offers the best opportunity to identify and tackle patterns of harmful behaviour in the creative industries. This behaviour can take place across multiple projects, organisations, productions and even sectors, reflecting the freelance workforce and project-based nature of so much creative work.

We have seen that this can make it difficult for any one organisation to see the wider picture or help prevent similar concerns from arising elsewhere. Sometimes these patterns of harmful behaviour have gone unchecked for years, creating avoidable distress.

By sharing appropriate information with CIISA as an independent, trusted body, you can help bring to light issues that may affect different workplaces, projects or sectors. You can also help us to act where harmful behaviour is recurring.

Your information can help us:

- spot emerging risks, repeated behaviour and wider workplace problems;
- understand how complaints and safeguarding concerns are handled;
- compare organisational learning with reports from workers, research and other sources;
- identify effective action and good practice; and
- recommend ways to make working environments across the creative industries safer, fairer and more respectful.

We know organisations will have questions about whether they can safely and lawfully report information to CIISA under UK data protection law. This guide answers many of the questions you may have to help you make that decision.

If you have any other questions you need answering before deciding whether to report, please contact us on whistleblowing@ciisa.org.uk

How is this different from whistleblowing?

Information given by an organisation is separate from a whistleblowing disclosure made by an individual worker. Both can provide valuable information, but their legal status and how CIISA records them are different.

Whistleblowing from an individual	Reports from organisations to CIISA
Made personally by a worker about wrongdoing they have experienced or witnessed through their work.	Made by an authorised representative on behalf of an organisation.
Issues may concern the worker personally but must also raise a wider public-interest concern to qualify for legal protection.	Shares information the organisation believes may help CIISA identify wider issues, patterns, themes or trends, and/or helps to protect workers, prevent harm, and improve safety at work in line with the CIISA Standards.

Whistleblowing from an individual	Reports from organisations to CIISA
May be protected under whistleblowing law from unfair treatment at work if the legal requirements are met.	Does not give organisations the same whistleblowing protections available to individual workers.
The individual shares information about themselves and others in confidence.	The organisation must ensure it has a lawful reason for sharing any information that contains personal details or could identify somebody.
Recorded and assessed as a potential whistleblowing disclosure under CIISA's prescribed-person process.	Recorded separately as organisational intelligence.
Included in CIISA's prescribed person reporting figures where the relevant legal requirements are met.	Recorded separately and is not included in CIISA's prescribed person reporting figures, but will be reported side-by-side.

Our organisation has an internal whistleblowing channel. Is this different from CIISA?

Yes. Your internal channel allows workers to raise concerns so that your organisation can investigate and take appropriate action.

CIISA provides an independent external whistleblowing reporting route, giving workers a choice of who to report to. Workers do not have to use an organisation's own whistleblowing route first before contacting us (for example, because a worker does not feel safe in using this internal route). However, we do not replace your internal process or act as an HR service or appeals body.

What CIISA does and does not do:

We:	We do not:
✓ help individuals and organisations understand what they can report to us	⊗ act on or respond to every concern raised
✓ consider when safeguarding action, support, signposting or a referral is needed in certain cases	⊗ resolve individual workplace disputes or act as an employer's HR service or appeals route
✓ use reports to identify emerging issues, patterns and trends	⊗ compel people to provide information or take enforcement action
✓ report on what we are seeing and recommend action	⊗ decide or assess whether your organisation has a lawful reason for sharing personal information with us;
✓ protect the confidentiality of reports and reporting people wherever possible.	⊗ provide legal advice;
	⊗ give detailed updates about every report we receive.

What can an organisation report to CIISA?

You can contact us about matters connected with the CIISA Standards or our wider work, including:

- issues, patterns or themes you have identified through complaints, whistleblowing channels, staff surveys or other workforce information;
- findings and learning from an internal investigation or review;
- safeguarding concerns or serious risks to workers that may have wider relevance across the creative industries;
- information originally raised by a worker or another organisation, where it is lawful and appropriate to share it with us;
- anonymised or aggregated information, research or sector intelligence; and
- effective practices or interventions that other organisations could learn from.

Is my organisation allowed to share information with CIISA?

Yes. Data protection law allows organisations to share personal information where there is a lawful, necessary and proportionate reason. This is known as having a ‘lawful basis’.

Your organisation must identify and record its lawful basis and share only the information needed.

We explain these requirements in more detail in Section 2.

If you are unsure whether you should share information with us, email whistleblowing@ciisa.org.uk.

What if it involves personal information about someone?

There may be times when an organisation may need to share necessary personal information about someone as part of their report.

Your organisation must identify and record why sharing the personal information is necessary. Section 2 explains what to consider, including the lawful bases that may apply.

2. Before you report

What do I need to consider when preparing a report for CIISA?

The following checklist is based on the ICO’s Data Sharing Code of Practice. It will help you decide what to share and record your reasons.

Your organisation is responsible for deciding whether it can share the information. CIISA is separately responsible for how it receives, stores and uses it.

Checklist	What to cover
1. Set out why you want to share	Be clear about what you want CIISA to understand and how sharing the information could help protect workers, prevent harm or improve creative-industry workplaces, and/or help CIISA in its wider work to monitor and embed the CIISA Standards.

Checklist	What to cover
2. Share only what is needed	Leave out information that is not relevant. Consider whether you can remove names, use broader dates or provide a summary instead of complete documents. Remember that someone may still be identifiable when different details are considered together.
3. Identify your lawful basis	Record which reason under data protection law allows you to share the information. This is known as your lawful basis. There are seven types in total. Depending on the circumstances, it might involve your organisation's legitimate interests, a legal duty, an official public function, protecting someone's life or freely given consent. We cover what each type may cover later in this guide.
4. Take extra care with sensitive information	Health, ethnicity, religion, trade-union membership, sexual orientation and similar information need extra protection. This is known as 'Special Category' data (see below). Separate rules also apply to criminal allegations, investigations and convictions.
5. Consider what people would expect	Think about whether sharing would be fair, whether it could cause unjustified harm and whether the people involved should be told. If you decide that the law allows you not to tell someone, record why.
6. Check whether anything else may prevent you sharing	Consider duties of confidentiality, contracts, court restrictions and any professional or regulatory rules. Take legal advice before sharing legally privileged material, as this may affect its protected status.
7. Describe the information accurately	Make clear what you consider is an allegation, an opinion, an internal finding or established fact. Describe where the information came from, when it was obtained and any important gaps or limitations.
8. Share it safely	Check that you are sending the information to the correct recipient, use CIISA's secure reporting route and limit access to people who need it. Contact CIISA first if there is any highly sensitive information that needs to be shared with additional security measures (encrypted or password protected).
9. Record your decision	Keep a short record explaining why you shared the information, what lawful basis and additional legal conditions you relied on, what information you shared and what safeguards you used.

Checklist	What to cover
10. Consider whether a more detailed assessment is needed	Complete a Data Protection Impact Assessment (DPIA) if the sharing is likely to create a high risk to people. If information will be shared regularly, CIISA and your organisation may want to have a written data-sharing agreement setting out what will be shared, why and how it will be protected.

Do we need the person's consent to share their personal information?

Not necessarily. Consent is one possible lawful basis, but it is only appropriate where the person has a genuine choice and can refuse or withdraw consent without disadvantage. Do not rely on consent if your organisation intends to share the information regardless.

Even where consent is not your lawful basis, consider the person's views and share only what is needed.

What are the different types of lawful basis?

There are seven types. **Annex A** lists each one and whether they may apply when reporting to CIISA.

What about sensitive information?

Some personal information needs extra consideration under data protection law because it is sensitive. This is known as **special category data** and includes information about a person's:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade-union membership;
- genetic data;
- biometric data used to identify them;
- health;
- sex life; or
- sexual orientation.

Before sharing this information with CIISA, your organisation should:

- consider whether sharing it is necessary;
- share only the information CIISA needs and anonymise it where possible;
- identify a lawful basis for sharing the personal information;
- identify an additional legal condition for sharing special-category data; and
- record the decision and any safeguards being used.

Some conditions also require an appropriate policy document explaining how the organisation protects and retains this information.

Separate rules apply to criminal-offence data. This includes information about alleged or suspected offences, investigations, proceedings and convictions. Your organisation will usually need both a lawful basis and an additional condition before sharing it.

If you are unsure, speak to your data protection lead or seek legal advice. You can also read the Information Commissioner's Office guidance on [special-category data](#) and [criminal-offence data](#), or call the ICO helpline on **0303 123 1113**.

You can also contact us at whistleblowing@ciisa.org.uk. We cannot provide legal advice or determine whether you can share this information with us, but we can explain what information CIISA needs and whether anonymised or less detailed information may be sufficient.

We are concerned that someone may bring a claim against us for sharing their information. What should we do?

Data protection law does not prevent appropriate information sharing, but your organisation is responsible for making sure its decision is lawful, fair and proportionate.

By following the checklist set out in this guide, carefully recording your reasons and lawful basis, and sharing only what is necessary will help demonstrate that you have followed the [Information Commissioner's Office Data Sharing Code of Practice](#).

These steps cannot prevent someone from making a complaint or claim. If you are uncertain about whether information can be shared, seek legal advice before doing so.

Will CIISA protect us from any claim if we share information with you?

Following the checklist, recording your lawful basis and sharing only what is necessary will help demonstrate that you have acted responsibly. Seek legal advice if you are uncertain.

CIISA does not provide a general indemnity. Your organisation remains responsible for its decision to disclose information. CIISA is separately responsible for how it handles the information after receiving it.

3. Making a report

How can I submit a report to you?

You can:

- ✓ Use CIISA's secure online reporting service [via our website](#);
- ✓ Email whistleblowing@ciisa.org.uk

What should we include?

What you include will depend on what is necessary for CIISA to understand the issue. Consider whether anonymised, aggregated or pseudonymised information would be sufficient.

Overall, please include:

- your organisation, role, and contact details;

- details of any other organisation, production or project involved (where relevant);
- details of what you want to report. Depending on the issue being reported, this could include specific details (such as what happened, when etc.) using the minimum personal data needed;
- details of any individuals associated with the report (only once you have carried out an assessment of whether you have a lawful basis to include personal information)
- whether the information is direct, second-hand, aggregated or based on an internal review;
- what action has already been taken and whether another process is continuing; and
- any immediate risk, safeguarding concern, or other issue you consider CIISA should be aware of.

Please tell us if you have anything that may be legally privileged, subject to a court restriction or may be particularly sensitive or confidential before sending it.

4. Our Process

What happens when we submit a report?

We will consider everything carefully, assess your report and consider how it can contribute to our understanding of issues across the creative industries. We take every report seriously.

We handle reports via the following steps:

Acknowledgement	We will confirm that we have received your report and explain what happens next. We will also provide information about privacy and available support.
Initial review	We aim to review new reports within 10 working days of receiving them. We consider whether it falls within our remit and raises any safeguarding, serious-risk or wider-industry issues Any immediate risk of serious harm will be considered without delay.
Assessment	We identify the main concerns, consider the information or evidence available and decide whether we need to ask you for anything further (where this is possible). We may also consider whether the information can be checked or supported by other sources.
Risk assessment	We consider any risks to the people involved. These may include whether there are any concerns about welfare and

	whether the issues raised require us to escalate how we handle the case.
Privacy Assessment	We protect personal information throughout our process. We consider who could be identified, whether sensitive information is involved and what safeguards are needed before information is used or shared.
Insight assessment	We consider whether the report reveals a new issue or adds to a theme, pattern or trend we are already seeing. Our level of confidence in the information helps us decide how it can be used; it is not a decision about whether an allegation is true or false.
Decision and review	We decide what should happen next. This may include recording and monitoring the concern, asking for more information, providing support or signposting, or considering an external referral or other action. Another senior member of staff reviews the decision to support fairness and consistency.
We aim to complete our initial assessment within one month of receiving your report. It may take longer if the report is complex or we need further information.	

Will you tell me what is happening with our report?

We will confirm that we have received your report. If you provide contact details, we may contact you if we need more information.

We cannot respond to or act on every individual report, so we may not provide further updates or tell you how the information has been used. However, every relevant report can help us identify wider issues, patterns and trends across the creative industries.

We may use information from your report as part of combined and/or anonymised insight without contacting you again.

If we think we would need more information for our insight reporting we will contact you to explain how we propose to use it and what steps we will protect identities.

We will not publish information in our insight reporting that could reasonably identify you/your organisation without discussing this with you first.

What happens in urgent or serious cases?

If a report suggests that someone may be at immediate risk of death, serious injury or harm, we will assess and escalate the concern without delay. This may include contacting the emergency

services, a safeguarding authority or another appropriate organisation where it is necessary and lawful to do so.

Other cases will be handled according to the level and nature of the risks identified. We may review our assessment if we receive new information or circumstances change.

Risk assessments support consistent decisions, but we consider each case individually and use professional judgment.

Will you contact others about our report?

We will not contact another organisation or person simply because you have made a report.

We may make contact where it is necessary to understand or check the information provided, address a safeguarding or serious safety risk, meet a legal requirement or take other proportionate action within our role.

Before doing so, we will consider:

- whether anyone could be identified;
- confidentiality and data protection;
- any effect on any legal action or HR process; and
- whether the contact is necessary and proportionate.

Where appropriate and possible, we will discuss this with you first. In limited circumstances, we may need to share information without your agreement, for example, where the law requires it or where sharing is necessary and proportionate to protect someone from serious harm.

Can we correct, update or ask you to delete our report?

Contact us if you need to correct or update your report. We may retain the original information and record the correction to maintain an accurate audit trail.

You may also ask us to delete information, but deletion is not automatic. CIISA is responsible for deciding what it needs to retain and why. Legal rights to correct or delete personal information belong to the individual concerned and do not necessarily require us to delete the whole report.

Requests concerning personal information can be sent to dpo@ciisa.org.uk

5. How we use the information you give

What we do will depend on a number of factors, such as whether the report falls within our remit, whether we need to act urgently, what information we have available, any privacy considerations, and what we can lawfully and proportionately do.

We may:

- **Record and monitor:** we decide to treat the report as a new issue - or link it to an existing issue, pattern or trend - and actively monitor what it tells us against existing and incoming reports.
- **Record and keep for internal reference:** We retain the information for future reference in case later reports indicate an emerging issue, pattern or trend.
- **Ask for more information:** If you have provided us with contact details, and are happy for us to contact you, we may ask you follow-up questions or ask for any evidence or other information, where possible and appropriate.
- **Provide support or signposting:** in serious and complex cases, where we can see there is more we can do to support you, we may direct you to a specialist support organisation that may be able to help.
- **Refer information externally:** We may share necessary information with an appropriate authority or specialist body where this is required by law or where there is another lawful, necessary and proportionate reason to do so, including to address a serious safeguarding or safety risk.
- **Take no further action on the individual report:** This may happen where the concern is outside our remit or cannot appropriately be progressed. Relevant information may still contribute to our wider understanding.

Safeguarding

If a report raises a possible safeguarding concern involving a child or an adult at risk, we will promptly consider whether safeguarding action or a referral is needed.

How do you decide whether information in a report contains important insight?

We do that by looking at two factors: insight confidence and significance.

Insight confidence

We assess how much confidence we can currently place in our understanding of the information. We consider:

- how clear, detailed and specific the report is;
- whether the important details are reasonably consistent;
- the relevance and reliability of any supporting information; and
- whether information could be checked against other reports or sources;

We may rate our current confidence as high, medium, low or undetermined. The rating is provisional and may change if we receive new information.

Our confidence rating is not a decision about whether the information in a report is true or false. A report will not be given a low rating simply because supporting documents or independent confirmation are not available.

Insight significance

Insight significance means how much the information may contribute to our wider understanding of how the CIISA Standards are being embedded in the creative industries.

We consider whether the report:

- raises a new issue;
- supports, adds to - or challenges - an issue we are already seeing;
- may indicate an emerging or established pattern or trend;
- has wider organisational, sector or strategic importance; or
- relates to relevant research or information from other organisations.

We may assess its current significance as high, medium, low or undetermined. As with insight confidence, this may change as we receive other reports or information.

We may consider that a report may be potentially significant even where information is currently limited. Equally, we may consider that a serious individual experience may have limited wider significance.

6. How we use insight

Do you use organisational reports in a different way?

We assess organisational reports alongside reports from individuals, other organisations, research and wider intelligence. This helps us identify new or repeated issues, decide what to monitor and build an evidence-led picture of how the CIISA Standards are being applied.

We use this information to identify risks and opportunities for improvement, we do not publish identifiable allegations about people or organisations.

We do this via four main stages:

Classify every report	We turn reports into structured insight by using a consistent way of recording data. This includes things like: • What sector or subsector is involved • Types of organisations, productions or projects • What key issues are being reported and how they are relevant to the CIISA Standards. • How we can use the report without identifying individuals or organisations
------------------------------	---

Identify and monitor patterns	We separate insight confidence and significance on each report so we can understand how well CIISA currently understands the issues, alongside how much the information could contribute to CIISA's wider work.
Build an evidence-led picture	We combine relevant reports and use our confidence and significance assessments to decide what should be prioritised, monitored or placed on an Insight Watchlist.
Report on what we are seeing	We consider whether the combined evidence is strong enough to report responsibly. We assess identification risks, seek appropriate approval and, where needed, obtain legal advice. We present findings fairly and focus on learning and improvement.

How will you protect named people and organisations when deciding whether to publish?

Our insight reports are designed to report on wider themes, patterns and trends using our analysis of information. We will not identify people or organisations in our public insight reports unless there is a lawful and justified reason to do so. We will anonymise or combine information to reduce the risk of identification.

In limited circumstances, we may have to disclose information confidentially where required by law or where this is necessary and proportionate to protect someone from serious harm. This is different from publishing information in our insight reports.

7. Privacy and confidentiality

For more information about our approach to privacy and confidentiality, the [CIISA Privacy Notice](#).

How do you protect our information when we report?

Access to organisational reports within CIISA is restricted to authorised people with a legitimate need to know. We carry out our own privacy assessment and may remove, separate or restrict information that is unnecessary or too risky to use.

We will consider any request for confidential treatment but cannot promise absolute confidentiality. This is because we may need to share necessary information where required by law or where there is another lawful, necessary and proportionate reason, including serious safeguarding or safety risk.

For every report we consider:

- what personal or sensitive information it contains;

- whether anyone could be identified directly or from a combination of details;
- any request for anonymity or restricted disclosure;
- whether linking the report with other information could reveal someone's identity;
- what information is necessary for our work;
- whether information can be removed, separated, redacted, anonymised or pseudonymised; and
- whether there is a lawful reason to use or share it.

Depending on the risks, we may apply our standard security controls, introduce additional safeguards or carry out a more detailed data-protection impact assessment before a proposed use of the information.

The privacy assessment may mean that information is used only internally, included only in an anonymised or aggregated form, or not used in any outward reporting.

Information being relevant or significant does not override our privacy and data-protection responsibilities.

What if an individual makes a subject access request to you about our report?

A person is entitled to their own personal information, not automatically to the full report or information about other people.

This means an individual may be entitled to any personal information your report includes about them. We will review the material carefully and may provide relevant extracts, a summary or a redacted copy rather than the report in full.

We will consider:

- the confidentiality of the report;
- the privacy and safety of reporters, witnesses and other people;
- whether disclosure could cause retaliation or other harm; and
- whether any legal exemption allows information to be withheld.

Where appropriate, we may consult your organisation before making a decision. However, CIISA remains responsible for responding to the request and your organisation cannot prevent disclosure where the law requires it.

Will this include letting the individual know where the report came from?

A subject access request may include a request for information about where someone's personal data came from.

An organisation's name is not normally personal data in its own right, so we cannot guarantee that your organisation will never be identified. Where appropriate, we may consult you before responding, but CIISA remains responsible for deciding what the law requires us to disclose.

If identifying your organisation would also identify a staff member, reporter or witness, we will consider whether it is reasonable and lawful to disclose that information. We may also withhold information where disclosure would prejudice a criminal investigation or reveal information that remains legally privileged.

8. Further Information

Can we ask CIISA for guidance about a specific matter?

Yes. You can ask how the CIISA Standards or our process may apply to a situation. We can identify relevant principles, questions and sources of specialist support.

You may make an enquiry using anonymised information. Only provide personal information where you have assessed that it is necessary and lawful.

Our guidance is general and non-binding. We cannot decide whether an allegation is true, determine an employment outcome or provide legal advice. If the enquiry reveals a serious risk or relevant intelligence, we may explain that it should also be treated as an organisational report.

I have further questions - can you help me?

For an enquiry about organisational reporting or guidance, email whistleblowing@ciisa.org.uk and we will do our best to answer any questions.

For any questions about data sharing or using personal information in a report, contact our Data Protection Officer on dpo@ciisa.org.uk.

The Information Commissioner's Office provide helpful guidance:

[ICO - Data sharing: a code of practice](#)

[ICO - Lawful basis for sharing personal data](#)

[ICO - Special category data](#)

[ICO - Criminal offence data](#)

[ICO - Data protection impact assessments](#)

This guide is a public summary of CIISA's procedural framework and is not legal advice.

Information accurate as of September 2026.

Annex A: Types of Lawful Basis and how they may apply when reporting to CIISA

Type	What this means	How this might apply when reporting to CIISA
Consent	The person has clearly agreed to their information being shared for a specific purpose. They can refuse or withdraw consent without being unfairly disadvantaged.	This may apply where the individual has been told specifically what will be shared with CIISA and why, has actively agreed, and can refuse without disadvantage.
Contract	Sharing the information is necessary to carry out a contract with the person.	This is unlikely to apply to most reports to CIISA. It may apply only where sharing the information is necessary to perform a contract with the individual.
Legal obligation	The organisation must share or use the information to comply with a specific legal duty.	This may apply where your organisation is under a specific legal duty to share the information with CIISA.
Vital interests	Sharing is necessary to protect someone's life.	This is normally limited to life-threatening emergencies where using the information is necessary to protect someone's life. CIISA is not an emergency service. If anybody is in immediate danger call 999.
Public task	Sharing is necessary for a public authority to carry out an official function or a task in the public interest that has a clear basis in law.	This may apply where a public authority or another organisation carrying out a legally based public function considers that reporting the information to CIISA is necessary as part of that function.
Legitimate interests	The organisation has a clear and reasonable reason for the sharing information with another organisation, and using personal information is necessary for that purpose. The benefit is not outweighed by unfair harm to the people involved.	This can apply where sharing to CIISA is necessary to help protect workers, prevent harm, improve workplace safety or help identify serious or repeated problems – or where sharing information would clearly assist CIISA's role in monitoring how the CIISA Standards are being applied across the creative industries. Sharing personal information is necessary to help CIISA carry out its official function as a prescribed person.
Recognised legitimate interest	The information may cover issues connected to a number of specific public-interest purposes, for which personal information may be used where necessary.	