Protected Disclosure (Whistleblowing) Policy

December 2024

Clear Channel Policy Control

Owner of this Policy:	**Head of Compliance, Clear Channel International**
Active Date:	**December 2024**
Questions on this Policy:	**compliance@clearchannel.com**

1. Operation of this Policy

This Policy has been developed in consultation with necessary stakeholders, is approved by the management of Clear Channel Outdoor Holdings, Inc. ("**Clear Channel**") and undergoes regular review to ensure compliance with applicable privacy and data protection legislation.

All Clear Channel Compliance policies support the operation of the **Clear Channel Code of Business Conduct and Ethics**.

The **Clear Channel Board of Directors** is ultimately responsible for ensuring that Clear Channel meets its obligations under this Policy, under the direction of the **Clear Channel Audit Committee**.

The **Head of Compliance** has day-to-day oversight of this Policy and maintains records of incidents around the Group which are reported to the Clear Channel Audit Committee on a quarterly basis. Should you identify any issues with the compatibility of this Policy and the rules in your jurisdiction, wish to discuss it, require any training or have concerns relating to this Policy, contact Compliance at compliance@clearchannelint.com.

1.1. Local Variations

You are expected to comply with both this Policy and any local variations of this Policy, where they are in force, as well as applicable laws and regulation, including those related to the subjects reportable under this Policy, Compliance programs and/or employment/labor laws ("**Applicable Laws**"). In some cases, Applicable Laws may be more restrictive than this Policy; where that is the case, the more restrictive rules must be followed.

1.2. Exceptions and Waivers

Local policies developed by Business Units must be in line with this Policy. All waiver or derogation requests to this Policy must be submitted in advance for approval by email to the Head of Compliance (compliance@clearchannelint.com) who has authority to grant a waiver or amendment at their discretion. Requests must allow sufficient time for meaningful review of the waiver request, and approval must not be assumed.

2. Introduction to this Policy

Clear Channel Outdoor Holdings, Inc., its affiliates and subsidiaries ("**Clear Channel**") are required to comply with Applicable Laws, its Code of Conduct and Company policies, and is committed to maintaining the highest standards of ethics, integrity, openness and accountability in its business operations.

To ensure such compliance and demonstrate its commitment to open and accountable management, Clear Channel have developed this Protected Disclosure (Whistleblowing) Policy ("**this Policy**"), providing Guidelines for making a Protected Disclosure.

3. What is a Protected Disclosure?

A **Protected Disclosure** is a disclosure of information relating to wrongdoing within the working environment or in a work-related context.

You may make a Protected Disclosure through Clear Channel's **Reporting Channels** as listed in **Section 6** where you reasonably believe that one or more of the following is happening, has taken place or is likely to happen in the future:

1. any suspected or identified violations of law and/or regulation including, but not limited to the commitment of a criminal offence (e.g., fraud), the breach of a legal obligation, and/or miscarriage of justice;
2. any forms of wrongdoing and serious misconduct that constitute an unlawful or unethical behavior within the working environment, including but not limited to suspected, or identified violations of policies, failure of a business process, and/or serious misconduct contrary to **Clear Channel's Code of Conduct and Business Ethics**; and/or
3. a danger to the health and safety of any individual or damage to the environment.

4. Who does this Policy apply to?

This Policy applies to anybody who decides to use Clear Channel's internal whistleblowing system to report certain forms of potential wrongdoing, from suspected or identified violations of Applicable Laws to breach of company policy and ethics frameworks, in accordance with this Policy and through Clear Channel Reporting Channels.

In particular, this Policy applies to:

1. **Internal Users** who acquired information on potential breaches in a work-related context relating to Clear Channel including the following:
    a. workers, contractors and those who work with Clear Channel on a self-employed basis, volunteers, and paid or unpaid trainees, and any persons working under the supervision and direction of contractors and subcontractors; and
    b. persons belonging to the administrative, management or supervisory body of Clear Channel, including non-executive members (together, "**Internal Users**").
2. **External Users** who report or publicly disclose information on potential breaches acquired in a work-based relationship:
    a. which has since ended;
    b. that includes breaches during the recruitment process or other pre-contractual negotiations where the work-based relationship is yet to begin;
    c. that are shareholders in our listed entities;

d. which are third parties who are connected with the reporter and who could suffer retaliation in a work-related context, such as colleagues or relatives of the reporter; and

e. which are legal entities that the reporter owns, work for or are otherwise connected with in a work-related context (together, "**External Users**").

NOTE! The Clear Channel Whistleblowing Hotline is not designed for use by members of the public or individuals who do not hold one of the above relationships with Clear Channel. Although other parties may under local legislation be permitted to report misconduct via the Whistleblowing Hotline, this Policy does not apply to any other party, including but not limited to customers, suppliers and third party data processors.

If you would like to express a concern or complaint and you are not an Internal User or an External User as defined above, please contact your Clear Channel relationship manager or compliance@clearchannelint.com.

Internal Users should follow the procedures set out in this Policy during their engagement or employment with Clear Channel and make a Protected Disclosure if they are concerned about any behavior that they witness, know about or think may amount to serious misconduct (as set out below).

5. Who is protected under this Policy?

Anybody to whom this Policy applies (see **Section 4**).

6. Which Clear Channel Reporting Channel do I use?

If you are an Internal User and you do not wish to speak to your manager or to a local representative of the Human Resources, Legal or Compliance Departments, we encourage you to use the following Clear Channel Reporting Channels as appropriate, depending on the nature of the serious misconduct you wish to report.[1] If you are still unsure, you may contact compliance@clearchannelint.com for assistance.

6.1. Clear Channel Internal User Reporting Channels for different categories of serious misconduct

Compliance Category	Description of Serious Misconduct	Clear Channel Reporting Channels
Fair Reporting (including financial and Sarbanes Oxley Act controls)	Theft, embezzlement, money laundering, tax evasion, accounting manipulation, any kind of financial fraud; financial or contract document forgery, non-compliance with financial regulation or internal control procedures. Any intentional misrepresentation of information, undue influence or independence concerns relating to interactions with external or internal auditors, or the oversight of audit functions of activities, including misstatement of revenues, misstatement of expenses, misstatement of assets, misapplications of accounting principles, or other wrongful transactions.	**Global Legal** at legal@clearchannelint.com **Global Compliance** at compliance@clearchannelint.com or via the **Whistleblowing Hotline** (see Appendix 1) or sending a written letter, addressed: **FAO Compliance** **33 Golden Square, London** **W1F 9JT**

[1] For Poland, there is also a mailbox in the copy room into which you can submit a written report.

Compliance Category	Description of Serious Misconduct	Clear Channel Reporting Channels
Fair Dealing (including economic crime controls)	Payments of bribery or facilitation payments to private individuals or public officials, corruption, improper sponsorships, donations, gifts and entertainment, violation of competition/ anti- trust laws or insider dealing; conflicts of interest, kickbacks, fraud, blackmail, misappropriation of company assets, falsification of contracts, reports or records.	**Global Legal** at legal@clearchannelint.com **Global Compliance** at compliance@clearchannelint.com or via the **Whistleblowing Hotline** (see Appendix 1) or sending a written letter, addressed: **FAO Compliance** **33 Golden Square, London** **W1F 9JT**
Fair Relationships (including human rights abuses)	Slavery, human trafficking, physical or mental abuse, discrimination or harassment due to a protected characteristic under law which is not handled by your local grievance policy, or retaliation for making a Protected Disclosure.	**Global Compliance** at compliance@clearchannelint.com or via the **Whistleblowing Hotline** (see Appendix 1) or sending a written letter, addressed: **FAO Compliance** **33 Golden Square, London** **W1F 9JT**
Workplace Violence	Workplace violence includes but is not limited to verbal or written abuse, stalking, harassment, physical attacks, fighting and unwelcomed physical touching; sexual or otherwise. This includes workplace violence committed by employees but also violence directed at employees by third parties including business partners, suppliers, customers, clients, students, or visitors; but also any persons who have no legitimate business at the worksite; violent acts by anyone who enters the workplace or approaches workers with the intent to commit a crime; violence against an employee by a present or former employee, supervisor, or manager; or violence committed in the workplace by a person who does not work there, but has or is known to have had a personal relationship with an employee.	CCO's Workplace Violence Prevention Plan; Legal at legal@clearchannel.com Employee Relations at MyHR@ClearChannel.com Global Compliance at compliance@clearchannel.com Reports via the Whistleblowing Hotline (see Appendix 1); or local equivalent contacts in CCE and CCLatAm or sending a written letter, addressed: **FAO Compliance** **33 Golden Square, London** **W1F 9JT**

Compliance Category	Description of Serious Misconduct	Clear Channel Reporting Channels
Fair Information Security	Data breaches, corporate espionage, computer viruses, sabotage or cybercrime.	You **must** first use the Information Security Team Breach Procedure for urgent matters on informationsecurity@clearchannelint.com
Fair Processing	A breach of data protection or privacy legislation.	The Privacy Office at mydata@clearchannelint.com
Fair Environment	Environmental pollution, serious failure to observe safe working practices, unsafe working conditions, and company violations affecting the health and safety of individuals at work. Violence or threats to personal safety.	A senior manager in your Business Unit or Clear Channel HQ; Your Business Unit Human Resources department; The Environmental Team at jade@clearchannelint.com or via the Whistleblowing Hotline (see Appendix 1).
Other Serious Misconduct	Other serious misconduct provided they relate to: a failure of a business process that may be systemic in nature; a crime or offence; a serious violation of laws, regulations or policy; a miscarriage of justice; or, if it poses a serious threat or damage to the public interest.	Your local or regional Legal Department (or Global Legal at legal@clearchannelint.com) Your Local Compliance Officer (or Global Compliance at compliance@clearchannelint.com) or, via the Whistleblowing Hotline (see Appendix 1) or sending a written letter, addressed: **FAO Compliance** **33 Golden Square, London** **W1F 9JT**
Other matters	For any concern concerning matters ordinarily dealt with under your grievance policy and Human Resources procedures, or any concern about business or strategic decisions taken by Clear Channel that do not include suspicions or allegations of serious misconduct.	• Your manager; • Your local Human Resources team; or • Senior Clear Channel management.

7. Can I report all types of Protected Disclosure through the Whistleblowing Hotline?

Some concerns are urgent. Whistleblowing Hotline reports may not reach us immediately. Therefore, **DO NOT** use the Whistleblowing Hotline to report:

- if your life is imminently in danger. Contact your local emergency services instead;
- information security breaches (which must go directly, and immediately, to informationsecurity@clearchannelint.com); or
- matters restricted by law in your country:
    - **Sweden**: Sweden permits reports only on 'key persons' in the company. We consider this to include anyone at least of manager level or higher.

For more information with regards to specific rules applying to your jurisdiction, please contact your Local Compliance Officer.

8. External reporting

External reporting channels for whistleblowing complaints vary depending on local laws.

More information on reporting concerns to external authorities can be found in Appendix 3.

9. Our obligations to you

Clear Channel will:

9.1. Investigate Protected Disclosures fairly

Where Clear Channel, in its discretion, determines that an investigation should be made, it will speak to relevant parties where appropriate, review facts impartially, and conduct the investigation in accordance with the **Clear Channel Investigations Protocol** and Applicable Laws.

Investigations may include internal or external resources with subject matter expertise, as necessary or appropriate. All Protected Disclosures will be held in confidence, and adequately secured. Clear Channel protects the identity of any whistleblower and shall not tolerate any retaliation against them.

9.2. Treat anonymous disclosures fairly

Clear Channel will always read anonymous disclosures, provided your country allows anonymous reporting (see **Section 7**).

However, Clear Channel encourages you to identify yourself while making a Protected Disclosure. Clear Channel will always protect the identity of whistleblowers. Knowing your identity will help Clear Channel to conduct an efficient and credible investigation.

Clear Channel may decide, in its reasonable discretion and after having conducted appropriate research, to limit its investigation of anonymous reports and not further proceed, if the serious misconduct reported upon in that anonymous report does not appear to be sufficiently serious, is vague or appears vexatious, does not contain supporting evidence, or there is no other corroborating evidence in support of the allegation. In such cases, Clear Channel will attempt to notify the individual who made the report of its decision to limit the investigation.

If you have any concerns about your identity being revealed, please contact the Head of Privacy here: mydata@clearchannelint.com.

9.3. Provide adequate safeguards for whistleblowers

Clear Channel will protect any whistleblowers who report their concerns under this Policy with reasonable grounds to believe that the report was true at the time it was made. Clear Channel will protect the privacy, identity and confidentiality of relevant parties, and will observe due process in respect of incriminated parties.

Your identity will not be disclosed to anyone, except, where disclosure is necessary (e.g. for: the proper investigation of the Protected Disclosure; legal reasons, disclosure to law enforcement agencies or regulatory bodies, the pursuance or defense of legal claims or the administration of justice); or with your consent.

Clear Channel will not tolerate the harassment, retaliation, or victimization of anyone raising a Protected Disclosure in good faith, and anyone responsible for detrimental conduct towards a whistleblower may be subject to disciplinary actions up to and including dismissal.

If you feel you have suffered any form of detriment for making a Protected Disclosure, it is important that you inform Compliance as soon as possible at compliance@clearchannelint.com.

9.4. Uphold any right to due process

Anyone implicated in a Protected Disclosure will be afforded due process in accordance with the laws of the jurisdiction in which they reside.[2] This is likely to include the presumption of innocence, until or unless Clear Channel in its discretion but acting reasonably, decides to take preventative, or disciplinary actions against an individual.

9.5. Protect Personal Data

Protecting the confidentiality, integrity and availability of your and others' **Personal Data** is important to Clear Channel. Personal Data obtained through the Protected Disclosure procedure will be processed in accordance with applicable Data Privacy Laws and Regulations.

10. Your obligations to Clear Channel

As part of Clear Channel, you are expected to:

10.1. Promptly let us know if you have concerns

We all have the obligation to operate ethically and within the law. To ensure compliance with its legal, regulatory and corporate obligations, Clear Channel requires all Internal Users and encouragers External Users to express concerns in relation to serious misconduct either confidentially or, if allowed by your jurisdiction, anonymously, and without fear of punishment or unfair treatment.

In most cases, we expect you to make a Protected Disclosure to us as soon as possible, and within three months of the act reported.

10.2. Make any disclosures in good faith

Any Internal User who maliciously and/or knowingly reported false or misleading information or, did not make the report in a timely manner could face disciplinary actions up to, and including termination.

[2] Poland requires either a searchable recording or a complete and accurate transcription of your conversation with the Whistleblowing Hotline.

External Users which make reports without reasonable grounds to believe in its truth are likely to lose any legal protection otherwise afforded under Whistleblowing Legislation.

10.3. Use the most appropriate Clear Channel Reporting Channel

Internal Users are encouraged to raise any concerns through your Business Unit's internal grievance and reporting procedures as listed in **Section 6**.

External Users should contact their relationship manager, or compliance@clearchannelint.com.

If that is not possible, both Internal Users and External Users are requested to promptly report the Protected Disclosure through the Hotline (see Appendix 1).

10.4. Do not retaliate against someone who makes a Protected Disclosure

If you become aware of a potential Protected Disclosure being made by another individual, either about you or other persons in Clear Channel, please contact compliance@clearchannelint.com for advice.

It is important that you do not retaliate against or cause detriment to that individual for making a complaint or raising a concern which is a potential Protected Disclosure. If you do, you may be subject to disciplinary actions up to and including termination.

11. What happens after I have made a Protected Disclosure?

If you have made a Protected Disclosure under your true identity, Clear Channel may contact you for more information.

Clear Channel will update you, where possible, on the progress of any investigation about a Protected Disclosure related to you within seven days, to the contact details provided by you. **Clear Channel will also provide feedback within three months of acknowledging your Protected Disclosure, if you have provided your contact details. However, depending on other legal requirements to which Clear Channel may be subject (including "Tipping Off" laws or privacy laws),** Clear Channel may not be able to grant access to, or notify, the individual(s) who made a Protected Disclosure, or suspected or implicated parties, of the full status, or content of the investigation being carried out.

If Clear Channel needs you to provide a witness statement, it shall notify you at the earliest opportunity.

12. Policy Control

Date of Last Review	Description of Major Changes	Reviewed/approved by (job role)
December 2024	Full review and update of Policy	Head of Compliance, CCI

Appendix 1: The Clear Channel Whistleblowing Hotline

What is the Whistleblowing Hotline?

The Whistleblowing Hotline is a confidential (or anonymous, where permitted by law), web and telephone-based reporting tool. It is maintained by an independent provider, Navex EthicsPoint.

Who do Whistleblowing Hotline Reports go to?

Protected Disclosures made through the Whistleblowing Hotline will be sent to the Clear Channel General Counsel, the Head of Compliance and the Audit Director. These individuals may delegate responsibility for investigating the Protected Disclosure in accordance with the Investigations Protocol.

How do I use the Whistleblowing Hotline?

There are two reporting facilities available via the Whistleblowing Hotline:

Option 1: Webpage Whistleblowing Hotline

You may submit an online report via the **EthicsPoint website: clearchannel.navexone.eu**.

If you wish, you may provide information in your native language, which will then be translated. You can also attach any evidence you have gathered in support of your Protected Disclosure using the upload function.

Option 2: Telephone Whistleblowing Hotline

You may prefer to make your report on the 'phone by speaking to a Navex call handler directly and confidentially in your local language by contacting the hotline telephone number next to your country below. If required your Protected Disclosure will be translated into English on your behalf. Navex call handlers will also be able to help you upload evidence in support of your Protected Disclosure or answer any procedural questions.

Certain numbers do not work from certain cell-phones due to in-country network provider restrictions. In that case, please use the online reporting tool.

Where can I get more information on the Whistleblowing Hotline?

For more information about the Whistleblowing Hotline, please read the **FAQs** on the Navex website (link here).

Hotline Online Link and Telephone Numbers

To report online:

clearchannel.navexone.eu/

To report by telephone:

Country	**Telephone numbers:** Each country has been allocated or a toll-free number or a 2-step direct access number		
Belgium	2 step	0-800-100-10, 0800-78755	Followed by 855-229-9304
Denmark	1 step	0-800-100-10, 80-251000	Followed by 855-229-9304
Estonia	2 step	800-12001	Followed by 855-229-9304
Finland	1 step	0800-9-15946	Followed by 0-800-11-0015, 855-229-9304
Ireland	1 step	1-800-550-000; 1-800-552-072	Followed by 855-229-9304; Ireland (UIFN) 00-800-222-55288
Latvia	2 step	(AT&T) 8000-2288	Followed by 855-229-9304
Lithuania	1 step	704-526-1128	
Netherlands	1 step	0800-0232214	
Northern Ireland	1 step	0808-234-7287	
Norway	1 step	800-12183	800-190-11, 855-229-9304
Poland	1 step	0-0-800-1510052	00-800-111-1111, 855-229-9304
Singapore	1 step	800-1102074	
Spain	2 step	900-99-0011, 999-971251	Followed by 855-229-9304
Sweden	1 step	020-79-8389	
Switzerland	2 step	0-800-890011, 0800-836085	Followed by 855-229-9304
UK	1 step	0808-234-7287	
US	1 step	001-844-715-9350	
Peru	2 step	(AT&T) 0800-50-288/000	Followed by 855-229-9304
Brazil	1 step	0800-892-0515	
Mexico	1 step	001-855-366-2458	
Chile	1 step	1230-020-1364	(Telmex – 800) 800-225-288
			(Telefonica) 800-800-288
			(ENTEL) 800-360-311
			(ENTEL - Spanish Operator) 800- 360-312
			(Easter Island) 800-800-311
			(Easter Island - Spanish Operator) at the English prompt dial 855-229-9304

Appendix 2: Glossary

Investigation Protocol	The Clear Channel Compliance document which sets out the procedures to be followed in investigations of Protected Disclosures, available on request from Compliance at compliance@clearchannelint.com.
Legitimate business reasons	These include tackling corporate crime involving Clear Channel, including fraud, corruption, tax or sanctions violations; protecting our business integrity and reputation; protecting and safeguarding our employees; and complying with regulatory and legal requirements including reporting obligations.
Local Compliance Officer (LCO)	The senior manager, usually the Legal Director or CFO, who is appointed to oversee Compliance in your Business Unit or region.
Personal Data	Any information relating to an identified or identifiable natural person, i.e. one who can be identified, directly or indirectly, by reference to an identifier: ID number, location data, online identifier, or factors specific to physical, physiological, genetic, mental, economic, cultural or social identity that relates to any subject that is in, or likely to come into, the possession of Clear Channel.

Appendix 3: Overview of Whistleblower Legislation

This Appendix sets out a high-level overview of the Whistleblower legislation in place across various markets in which Clear Channel operates and outlines competent authorities to which external reports may be made where an individual is unsatisfied with Clear Channel's internal reporting system. Please note that this list is not exhaustive and other whistleblowing protections and reporting provisions may exist in local/provincial laws that are not included in this Appendix.

Should you require more detail as to your local Whistleblowing laws and external reporting channels, please consult the Clear Channel Compliance team (compliance@clearchannelint.com).

A3.1. Whistleblowing laws and external reporting channels applicable to our European markets

Country	Whistleblowing legislation	External coordinating bodies / competent authorities
Belgium	The Belgian Act on the protection of persons who report breaches of national or Union law	The Federal Ombudsman
Denmark	The Danish Whistleblower Protection Act	The Danish Data Protection Authority
Estonia	Whistleblower Protection Act	TBC: A specified authority is yet to be designated
Finland	Whistleblower Protection Law 1171/2022	Office of the Chancellor of Justice
Ireland	The Protected Disclosures (Amendment) Act 2022	The Office of the Protected Disclosures Commissioner (OPDC)
Latvia	Whistleblowing Act	Whistleblowers' Contact Point at the State Chancellery
Lithuania	Law on the Protection of Whistleblowers of the Republic of Lithuania	The Public Prosecutor's Office of the Republic of Lithuania
Netherlands	The Dutch Whistleblowers Act	The Whistleblowers' House
Norway	Norwegian Working Environment Act (WEA) (Chapter 2A) ***NB: Applies to employees only***	Varies depending on issue. There are several public supervisory authorities amenable to reports, such as the Norwegian Labour Authority, the police and the Data Protection Authority.
Poland	The Act on the Protection of Whistleblowers	The Commissioner for Human Rights (the Ombudsman)
Spain	Whistleblowing Law 2/2023	The Independent Authority for the Protection of Whistleblowers (AAI)
Sweden	The (new) Swedish Whistleblower Act (SFS 2021:890)	The Swedish Work Environment Authority is the key competent authority. Other authorities appointed for specific sectors include the Swedish Financial Supervisory Authority and the Swedish Authority for Privacy Protection.
UK	Public Interest Disclosure Act 1998	Varies depending on issue. For example, the Information Commissioner for data protection concerns or the Environment Agency for environmental concerns.

A3.2. Whistleblowing laws and external reporting channels applicable to our Latin American markets

Country	Whistleblowing legislation	External coordinating bodies / competent authorities
Brazil	Brazilian Anticrime Law (Article 15 of Federal Law 13.964/2019) Victim and Witness Protection Act (Federal Law 9.807/1999)	Varies depending on issue. Includes Administrative Council for Economic Defence (CADE) and the public prosecution service.
Chile	Law No. 20,393 / Decree Law No. 2 of 1976	Labour Board or the Courts
Mexico	TBC	TBC
Peru	Law N° 30424 / Legislative Decree 1327 (Article 2)	Office of Institutional Integrity

A3.3. Whistleblowing laws and external reporting channels applicable to our US markets

Country	Whistleblowing legislation	External coordinating bodies / competent authorities
US	Whistleblower Protection Act of 1989	SEC – Office of the Whistleblower