Protected Disclosure (Whistleblowing) Policy

Clear Channel

Protected Disclosure (Whistleblowing Policy

Owner of this Policy:	Clear Channel Outdoor Holdings, Inc. Chief Compliance Officer
Active Date:	6 December 2021
Queries on this Charter:	contact compliance@clearchannelint.com

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 Conduct and Business 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 **Chief Compliance Officer** has day to day oversight of this Policy. Should You identify any issues with the compatibility of this Policy and the rules in your jurisdiction, wish to discuss it, or have training or concerns relating to this Policy, contact Compliance at compliance@clearchannelint.com.

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.

Exceptions and Waivers.

Local policies developed by Business Units must be in line with this Policy. Any request for a waiver or amendment of this Policy must be submitted by email to the Clear Channel Chief Compliance Officer (compliance@clearchannelint.com) who has authority to grant a waiver or amendment at his/her discretion.

PROTECTED DISCLOSURE (WHISTLEBLOWING) POLICY

1. Introduction to this Policy.

Clear Channel Outdoor Holdings, Inc, its affiliates and subsidiaries (''**Clear Channel**'') are required to comply with applicable laws and regulations, 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.**

2. 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 Disclosures through Clear Channel's Reporting Channels 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, miscarriage of justice etc.;
2. any forms of wrongdoing and serious misconduct that constitute an unlawful or unethical behaviour within the working environment, such as suspected, or identified violations of policies, failure of a business process, serious misconduct contrary to **Clear Channel's Code of Conduct and Business Ethics etc.** and**/**or;

3. a danger to the health and safety of any individual, or damage to the environment.

3. To whom does this Policy apply?

This Policy applies to anybody who decides to use Clear Channel's internal whistle-blowing system to report certain forms of wrongdoing, from suspected or identified violations of applicable laws and regulations 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 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 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 within 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").

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.

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 your engagement or employment with Clear Channel and make a Protected Disclosure if you are concerned about any behaviour that you witness or know about, that you think amounts to serious misconduct (as set out below).

4. Who is protected under this Policy?

Anybody to whom this Policy applies.

5. 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. If you are still unsure, you may contact compliance@clearchannelint.com for assistance.

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

Compliance Category	Description of Serious Misconduct	Clear Channel Reporting Channel
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).
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,	Global Legal at legal@clearchannelint.com Global Compliance at compliance@clearchannelint.com; or

	kickbacks, fraud, blackmail, misappropriation of company assets, falsification of contracts, reports or records.	via the Whistleblowing Hotline (see Appendix 1).
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).
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).
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; Senior Clear Channel management.

6. May I report any 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.
- Information security breaches (which must go directly, and immediately, to informationsecurity@clearchannelint.com); or
- matters restricted by law in your country:

    a. **Sweden:** Sweden permits reports only on 'key persons' in the company. We consider this to include anyone at least of manager level or higher;

b. **France:** Anonymous reports shall be exceptional and handled with specific guarantees (establishment of the seriousness of the reported violation, existence of detailed factual elements and prior exam by the by the first recipient of the report before the initiation of further investigations).

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

7. 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.

8. Our obligations to you.

Clear Channel will:

✓ 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 and Regulations.

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.

✓ Treat anonymous disclosures fairly.

✓ Clear Channel will always read anonymous disclosures, provided your country allows anonymous reporting (Portugal does not permit anonymous reports, while France has implemented special rules for anonymity (see **section 6**).

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 an 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 Chief Data Privacy Officer here: mydata@clearchannelint.com

✓ Provide adequate safeguards for whistle-blowers.

Clear Channel will protect any whistle-blowers 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 defence of legal claims or the administration of justice); or with your consent.

Clear Channel will not tolerate the harassment, retaliation, or victimisation 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.

✓ **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. 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.

✓ **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.

9. Your obligations to Clear Channel.

DO:

✓ **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.

✓ **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.

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.

✓ **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 5, above.

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 One).

✓ **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 cause detriment to that individual for making a complaint or raising a concern. If you do, you may be subject to disciplinary actions up to, and including termination.

10. 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 endeavour to update you, where possible, on the progress of any investigation about a Protected Disclosure related to you. However, 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 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.

APPENDIX 1

The Clear Channel 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 Chief Compliance Officer 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:

- **Webpage Whistleblowing Hotline**

  You may submit an online report via the **EthicsPoint web link**

  (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.

- **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.

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

Hotline telephone numbers

Report Online (Global):	clearchannel.navexone.eu/		
Country	**Telephone numbers:** **Each country has been allocated 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
France	1 step	0800-917075	
Ireland	1 step	1-800-550-000; 1-800-552-072	Followed by 855-229-9304; Ireland (UIFN) 00-800-222-55288
Italy	1 step	800-797458	800-172-444, 855-229-9304
Latvia	2 step	(At&T) 8000-2288	Followed by 855-229-9304
Lithuania	1 step	704-526-1128	
The 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	Chile (Telmex – 800) 800-225-288 Chile (Telefonica) 800-800-288 Chile (ENTEL) 800-360-311 Chile(ENTEL - Spanish Operator) 800-360-312 Chile (Easter Island) 800-800-311 Chile(Easter Island - Spanish Operator At the English prompt dial 855-229-9304

APPENDIX 2

Glossary

Investigation Protocol means 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: includes 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): means the senior manager, usually the Legal Director or CFO, who is appointed to oversee Compliance in your Business Unit or region.

Personal Data: means 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

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[1]. 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)

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	Federal Ombudsman
Denmark	The Danish Whistleblower Protection Act	Varies depending on issue. For example, privacy concerns may be reported to the Danish Data Protection Authority
Estonia	TBC	TBC
Finland	Whistleblower Protection Law 1171/2022	Office of the Chancellor of Justice
France	Decree n°2022-1686 (the French Whistleblowing Legislation)	Defender of Rights
Ireland	The Protected Disclosures (Amendment) Act 2022	The Office of the Protected Disclosures Commissioner (OPDC)
Italy	Decree no. 24/2023 (the Italian Whistleblowing Legislation)	National Anti-Corruption Authority (ANAC)
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 Dutch Whistleblowers Authority
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 Polish Act on the Protection of Persons Who Report Breaches of Law - TBC	The Polish Ombudsman – TBC
Spain	Whistleblowing Law 2/2023	Independent Authority for the Protection of Whistleblowers (AAI)
Sweden	The (new) Swedish Whistleblower Act (SFS 2021:890)	Multiple competent authorities including the Swedish Financial Supervisory Authority, Swedish Authority for Privacy Protection, and Swedish Work Environment Authority.

[1] *As of 6th April 2023 (date of drafting)*

UK	Public Interest Disclosure Act 1998	Varies by issue. For example, concerns regarding data protection or the environment can be made to the Information Commissioner or Environment Agency respectively

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 by 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

Whistleblowing laws and external reporting channels applicable to our US market

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