SM GROUP INTERNAL INFORMATION SYSTEM POLICY

Index

1. DEFINITIONS

The definitions of the concepts that will be used frequently in this document are listed below.

Definitions related to the organizational structure of Grupo SM:

- **Grupo SM / the Organization**: includes the entities that adhere to this Policy, as well as the Grupo SM Internal Information System Management Procedure, which are listed in **Annex I**.
- **Ethics Committee:** internal body of Grupo SM responsible for the duties set out in the Code of Ethics.
- **Governing Body**: administrative or governing body of the corresponding SM Group entity.
- **Members of the Organization** : members of the Governing Bodies, Senior Management, executives, employees (full-time or temporary employees or those under collaboration agreements), volunteers of the Organization, and all other persons under the hierarchical authority of the above in any of the entities that make up Grupo SM.
- Senior **Management**: persons responsible for managing and controlling Grupo SM at the highest level, i.e., reporting directly to the Governing Body.
- **Third Party**: a natural or legal person outside the Organization or an independent body with which the Organization has a relationship.

Definitions related to the SM Group's internal information system:

- **Internal information system**: internal system that integrates the various internal information channels of Grupo SM and allows for the secure submission of communications.
- **Internal information channels**: reporting and internal communication mechanisms integrated into the SM Group's internal information system.
- **Head of the Internal Information System**: body appointed by the Governing Body, responsible for managing the SM Group's Internal Information System independently and autonomously.

- **Communication**: communication relating to a breach (active or omissive behavior) of the regulations applicable to Grupo SM, occurring in a work or professional context. In particular, the following breaches shall be understood to be reportable through the Internal Information System:
  - Violations of applicable legislation relating, among other things, to the following areas: public procurement, the financial sector, the prevention of money laundering or terrorist financing, product safety and conformity, transport safety, environmental protection, radiation protection and nuclear safety, food and feed safety, animal health and welfare, public health, consumer protection, privacy and personal data protection, and network and information system security.
  - Serious or very serious criminal or administrative offenses.
- **Whistleblower**: a person who files a report or makes a public disclosure (subject to the conditions set out in section 7 of this Policy). The term "whistleblower" includes not only public employees or employees, but also all self-employed workers, shareholders, partners, and members of the company's governing, management, or supervisory body, persons working for or under the supervision of contractors, subcontractors, or suppliers, volunteers, interns, and workers in training, as well as persons whose employment or statutory relationship has ended or has not yet begun.
- **Related third parties**: this includes those persons within the organization who assist the whistleblower in the process, as well as related persons who may suffer reprisals, such as co-workers or family members.
- **Person affected by the report**: natural or legal person or persons to whom a report of an alleged infringement is attributed.
- **Procedure for managing communications received by Grupo SM**: Grupo SM's internal regulations establishing the essential rules for managing communications received through the channels that make up the internal information system.

2. PURPOSE

This Policy sets out the principles governing the SM Group's internal reporting system, which is **the preferred channel for reporting actions or omissions**, which will in all cases **be dealt with effectively** by the Organization.

As a sign of its **commitment to a culture of ethics and compliance**, the SM Group's Governing Body, after consulting with the workers' legal representatives, has implemented an Internal Reporting System and approved this Policy, with the aim of establishing a standard of protection for Whistleblowers.

This Policy has been developed in accordance with the following regulations applicable in Spain, without prejudice to its enforceability in all jurisdictions where Grupo SM is present:

- **Law 2/2023, of February 20,** regulating the protection of persons who report regulatory violations and the fight against corruption.
- **Directive (EU) 2019/1937** of the European Parliament and of the Council of October 23, 2019.
- **LDE**: Law 1/2019, of February 20, on Trade Secrets.
- **GDPR**: Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
- **LOPDGDD**: Organic Law 3/2018, of December 5, on the Protection of Personal Data and Guarantee of Digital Rights.
- **Organic Law 7/2021**, of May 26, on the protection of personal data processed for the purposes of prevention, detection, investigation, and prosecution of criminal offenses and the execution of criminal penalties.
- **TFEU**: Treaty on the Functioning of the European Union.
- **ISO 37002:2021 standard on whistleblowing management systems.**

3. SCOPE

This Policy is mandatory and applicable to all entities that make up Grupo SM in accordance with the definition in section 1 thereof, which adhere to it through their respective governing bodies. It is therefore applicable to all members of the Organization, regardless of their position or geographical location.

For the purposes of formally adhering to the internal reporting system, the various entities of Grupo SM, which are listed in **Annex I** to this document, must obtain formal approval from the governing body of the respective entity, as provided for in section 12 of this Policy.

The various protection measures provided for in this Policy shall be exercised, as appropriate, on all Whistleblowers, Related Third Parties, and Persons Affected by the Communication.

This channel will allow for the communication of, including but not limited to, the following behaviors:

- Harassment, hostile or offensive conduct.
- Actions related to possible irregularities in relations with suppliers and/or purchases.
- Actions related to public and private corruption.
- Misappropriation and diversion of resources.
- Money laundering.
- Accounting irregularities and inaccuracies.
- Conflict of interest.
- Improper commitments to third parties.
- Falsification of documents, contracts, reports, or records.
- Violation of employee rights or breaches of the applicable collective bargaining agreement.
- Violations of Grupo SM's existing policies and procedures regarding information security.
- Any behavior that involves improper conduct and irregularities contrary to the values and principles that govern Grupo SM. In short, any behavior that could contravene applicable regulations, the Code of Conduct, or Grupo SM's internal policies and procedures.

In the case of an employment or professional relationship, the facts may relate to a relationship that is (i) still in force, (ii) already terminated, or (iii) not yet initiated (for example, if it refers to violations relating to selection processes or pre-contractual negotiations).

4. HEAD OF THE SM GROUP INTERNAL INFORMATION SYSTEM

In order to ensure the supervision and proper compliance of the Internal Reporting System, Grupo SM has appointed the Grupo SM Ethics Committee as the System Manager. The Committee has the appropriate competence, integrity, authority, and independence, as well as the necessary resources to perform its functions.

The Ethics Committee, as a collegiate body, is composed of the following individuals:

- Vice President of SM.
- Director of Internal Audit.
- Corporate Director of People.
- Corporate Director of Operations.
- Director of Corporate Legal Affairs.

The powers of management of the System and of processing investigation files within the Ethics Committee fall to the Corporate Director of People.

The exchange of information between the different entities of the group shall be admissible for the proper coordination and best performance of their functions.

Likewise, for the purposes of achieving adequate management of the internal information system, the collaboration of the Ethics Delegates appointed in each country is expressly provided for in the event that this is required by the Ethics Committee and/or the Corporate Director of People.

Both the appointment and dismissal of the individually designated natural person, as well as the members of the collegiate body, shall be notified to the Independent Whistleblower Protection Authority (A.A.I.) within ten business days, specifying, in the case of dismissal, the reasons that justified it.

5. INTERNAL CHANNELS INTEGRATED INTO THE SM GROUP'S INTERNAL INFORMATION SYSTEM

Through this Policy, Grupo SM integrates the various internal information channels available to the Organization. Thus, the various internal information channels that make up the System guarantee the principles and safeguards of Whistleblowers, Related Third Parties, and Persons Affected by the Communication. Any Communications may be submitted either **anonymously or by name**.

In any case, the Communication will be managed in accordance with the terms described in the SM Group's Internal Information System Management Procedure.

Grupo SM will ensure that the channels integrated into the Internal Information System are secure, complying with applicable personal data protection regulations and guaranteeing the rights of Whistleblowers, Related Third Parties, and Persons Affected by the Communication, as well as their confidentiality. Similarly, Grupo SM will ensure that no reprisals are taken against them when they use the communication channels in good faith.

Thus, this Policy is applicable to anything not expressly provided for in the harassment protocols or other specific protocols approved in the various entities of Grupo SM. In this regard, Communications received in relation to these Protocols will be managed in accordance with the terms established in the Grupo SM Internal Information System Management Procedure.

5.1. TOOL AND MECHANISMS FOR FORMULATING COMMUNICATIONS

Grupo SM has adopted an internal communications channel through a computer *tool—Whistleblower Software* APS—owned by an external third party, in order to (i) guarantee the effectiveness of organizational and management models in the prevention of criminal risks; (ii) reinforce the appropriate surveillance and control measures for the prevention of criminal activities within Grupo SM; and (iii) comply with the utmost reliability with the obligations set forth in current regulations.

The platform can be accessed from any device with an internet connection via the following link:

https://whistleblowersoftware.com/secure/smcanalinterno

The communication will be handled in accordance with the terms described in the SM Group Internal Information System Management Procedure.

In addition, the SM Group's Internal Information System provides for the possibility, at the request of the whistleblower, of submitting a communication through a face-to-face or telematic meeting, which must be held within a maximum period of seven (7) days from the request made by the whistleblower.

Communications presented at a face-to-face or telematic meeting will be managed in accordance with the provisions of the SM Group's Internal Information System Management Procedure**.**

6. PRINCIPLES OF THE INTERNAL INFORMATION SYSTEM

PRINCIPLE OF INDEPENDENCE

The procedures arising from the various Communications shall be governed with the utmost independence, with the SM Group Internal Information System Management Procedure establishing the corresponding mechanisms to avoid any conflicts of interest.

PRINCIPLE OF OBJECTIVITY AND IMPARTIALITY

The investigation of cases arising from Communications submitted through the various information channels shall be governed in all cases by the principles of objectivity and impartiality.

PRINCIPLE OF PROPORTIONALITY

The investigation measures, the proposed action by the System Manager, and the preliminary measures that may be agreed upon during the investigation, in accordance with the terms set out in the SM Group Internal Information System Management Procedure, will be evaluated in all cases taking into consideration the principle of proportionality.

PRINCIPLE OF CONFIDENTIALITY

Grupo SM guarantees the utmost confidentiality of the Communications received and their content, in accordance with the provisions of section 7.4 of this Policy and section 4.5 of the Grupo SM Internal Information System Management Procedure, among others.

PRINCIPLE OF PROHIBITION OF RETALIATION

It is strictly prohibited to take any action against any person who uses the internal reporting channels that constitutes retaliation or has negative consequences, on the grounds of having made a report in the proper manner and in accordance with the conditions of use of the Internal Reporting System.

7. PROTECTION PARAMETERS

7.1. PERSONS ELIGIBLE FOR PROTECTION

Grupo SM will provide protection to both the Whistleblower acting in good faith and related Third Parties against any harm they may suffer as a result of reporting possible violations of which they have become aware.

Likewise, Grupo SM will extend protection, under the terms legally provided for in this case, to the persons affected by the report.

7.2. CONDITIONS OF PROTECTION

A whistleblower acting in good faith is considered to be someone who, at the time of making the report, has at least some reason and evidence to reasonably think or doubt the need to clarify the veracity of the risks and breaches that they may have noticed through the internal reporting system, without the need to provide conclusive evidence.

Persons whose Communication meets any of the following conditions are **expressly excluded** from the protection granted by the SM Group's internal information system:

- Information contained in communications that have previously been rejected by any other internal communication channel of the system, such that the information contained therein has already been evaluated or resolved. The foregoing is provided that no additional or new facts or evidence are provided.
- Information whose facts are not covered by the definition of Communication provided in section 1 of this Policy. By way of example, Communications relating to interpersonal conflicts or which constitute mere rumors are excluded from the protection granted to the Whistleblower.

7.3. CASES OF PUBLIC DISCLOSURE

In the event that the Whistleblower makes a **public disclosure**, in order to be eligible for protection, they must also meet one of the following special conditions for protection:

- They must have first made the communication through internal and external channels, or directly through external channels.

- They have reasonable grounds to believe that the violation may constitute an imminent or manifest danger to the public interest; or, in the case of communication through an external information channel, there is a risk of retaliation or there is little likelihood that the information will be dealt with effectively due to the particular circumstances of the case, such as the concealment or destruction of evidence, collusion between an authority and the perpetrator of the infringement, or the involvement of the authority in the infringement.
- The conditions for protection set out in the previous section shall not apply when the person has disclosed information directly to the press in accordance with the exercise of freedom of expression and accurate information as provided for in the Constitution and in its implementing legislation.

Public disclosure shall be understood to mean making information on the actions included in section 3 of this Policy available to the public.

7.4. MEASURES TO PROTECT WHISTLEBLOWERS AND RELATED THIRD PARTIES

Grupo SM is responsible for ensuring the protection of Whistleblowers and Related Third Parties. The System Manager is responsible for ensuring that these protection measures are effectively implemented within the Organization.

PROHIBITION OF RETALIATION

All Members of the Organization are strictly prohibited from retaliating against Whistleblowers acting in good faith, including threats of retaliation and attempts at retaliation.

Retaliation is understood to mean any act or omission that is prohibited by law or that, directly or indirectly, involves unfavorable treatment that places the persons suffering it at a particular disadvantage in relation to others in the workplace or professional context, solely because of their status as Whistleblowers or Related Third Parties, or because they have made a public disclosure.

If Grupo SM becomes aware that retaliation is occurring or has occurred, it will take reasonable measures to stop and address it. In this regard, the situation of the

Whistleblower or Related Third Party will be remedied as if they had not suffered retaliation. For example:

a) Reinstate the person to the same or equivalent position, with the same salary, responsibilities, job status, and reputation.
b) Allow equal access to promotion, training, opportunities, benefits, and rights.
c) Restore the person to their previous commercial position in relation to the Organization.
d) Cease or withdraw any conflict or litigation that may exist against the person (e.g., attitude or treatment offered).
e) Apologize for any harm suffered.

CONFIDENTIALITY AND PROTECTION OF PERSONAL DATA

Grupo SM has an obligation to preserve the identity of the Whistleblower and related Third Parties, as well as to guarantee the confidential treatment of their data.

In this regard, the internal information system is designed, established, and managed in a secure manner, so as to guarantee the confidentiality of the identity of the Whistleblower and any third party mentioned in the Communication, and of the actions carried out in the management and processing thereof, as well as the protection of data, preventing access by unauthorized personnel.

Grupo SM undertakes not to process personal data that is not necessary for the knowledge of the actions or omissions reported in the communications indexed in the Internal Information System and that does not also have the appropriate legal justification; in this case, the data will be deleted.

Three (3) months after receiving the Communication without any investigation having been initiated, Grupo SM will proceed to delete it, unless the purpose of its retention is to leave evidence of the functioning of the System. In the latter case, the information must be anonymized. Likewise, Grupo SM will not retain personal data for a period exceeding ten (10) years.

In short, the Organization undertakes to comply with the deadlines established in the applicable regulations and in the SM Group's Internal Information System Management Procedure.

7.5. PROTECTION MEASURES FOR PERSONS AFFECTED BY THE COMMUNICATION

The main protection measures that will be implemented for persons affected by the communication are as follows:

a) Right to the presumption of innocence.
b) Right to defense.
c) Right of access to the case file.
d) Protection of your identity, guaranteeing the confidentiality of the facts and data of the proceedings.
e) Comply with the deadlines established in the applicable regulations and in the SM Group's Internal Information System Management Procedure.

The scope of these measures will be limited by the specificities that, depending on each type of Communication or its subject matter, are applicable under current legislation.

7.6. ACTIVATION OF PROTECTION

The measures to protect the Whistleblower, related Third Parties, and Persons affected by the Report will be activated and will begin as soon as the report is received, and will continue during and even after—when necessary—the conclusion of the investigation or management of the Report.

8. TRAINING

The Governing Body, the System Manager, the Ethics Committee, the SM Group Ethics Delegates in each country, as well as any other person who has roles, responsibilities, and authority within the Internal Reporting System, or who is likely to receive Reports due to their position, must be trained on how to operate this Policy and the SM Group Internal Reporting System Management Procedure.

This training shall include, among other aspects, the guarantee of confidentiality that must prevail, the warning that any breach is classified as a very serious offense, and the establishment of the obligation of the recipient to immediately forward the information received to the System Manager.

9. CONSEQUENCES OF NON-COMPLIANCE

All persons covered by this document are obliged to comply with its contents. In the event of a serious breach being identified, the Internal Information System shall be the preferred channel for reporting such breach.

When a violation of the Code of Ethics and this Policy is investigated and confirmed, disciplinary measures (in the workplace) or contractual measures (in commercial relations with third parties) will be taken that are considered proportional to the risk or damage caused.

The measures adopted from an employment perspective will comply with applicable regulations, without losing their forcefulness or proportionality to the seriousness of the events that gave rise to them, informing the workers' legal representatives if appropriate.

If the accusations described in the Communication are found to be false or malicious, to the extent that they have been made deliberately with knowledge of their falsity or recklessly, they will be considered a serious breach of the SM Group's Internal Information System Management Policy and Procedure.

Based on the above, Grupo SM shall be entitled, in compliance with applicable labor regulations and contracts signed in the case of professionals, to take any of the actions set out in section 6 of the Grupo SM Internal Information System Management Procedure.

10. ADVERTISING

This Policy is available to all Members of the Organization and Third Parties through its publication on the following internal information channel:

https://whistleblowersoftware.com/secure/smcanalinterno

Grupo SM undertakes to disseminate and bring to the attention of all Members of the Organization the information necessary to understand the Internal Information System, its principles, guarantees, and obligations, as well as its preventive purpose. In this regard, the Policy is also accessible through the employee portal, in the "Information, documents, and procedures" section, under "Policies and procedures."

People Space

11. ADHERENCE OF GRUPO SM ENTITIES TO THE INTERNAL INFORMATION SYSTEM

This Policy and the Management Procedure for the SM Group's Internal Information System is mandatory for all entities within the SM Group under the terms established in section 1.

In this regard, the governing bodies of the entities that make up the SM Group shall expressly adhere to this policy.

12. ENTRY INTO FORCE AND AMENDMENTS

The Internal Information System Policy shall enter into force on the day following its approval. This Policy will be reviewed if possible improvements are identified or if regulatory, organizational, or any other changes occur that justify such a review.

ANNEX I: SM GROUP INTERNAL INFORMATION SYSTEM POLICY

Nombre empresa	País
COMBOIO DE CORDA EDITORA, LTDA.	Brasil
EDIÇÕES SM, LTDA.	Brasil
EDITORA ANZOL, LTDA	Brasil
EDITORA MOITARÁ, LTDA.	Brasil
EDITORA RODOPIO, LTDA.	Brasil
EDITORA TIMBÓ, LTDA.	Brasil
FUNDACIÓN ATE CHILE, S.A.	Chile
INSTITUTO IDEA CHILE, S.A.	Chile
SM, S.A.	Chile
UD PUBLISHING CHILE, SpA	Chile
COMERCIALIZADORA PPC, S.A.S.	Colombia
EDICIONES PPC, S.A.S.	Colombia
SM EDUCACIÓN, S.A.	Colombia
ACENTO EDUCACIÓN, S.A.	España
COMERCIAL DE EDICIONES SM, S.A.U.	España
EDITORIAL CRUÏLLA, S.A.	España
FUNDACIÓN SANTA MARÍA	España
GRUPO EDITORIAL SM INTERNACIONAL, S.L.	España
IKASMINA ARGITALETXEA, S.L.	España
PPC EDITORIAL Y DISTRIBUIDORA, S.A.	España
XERME EDICIONS, S.L.	España
ASESORÍA EN TECNOLOGÍAS Y GESTIÓN EDUCATIVA, S.A. DE C.V.	México
MÉXICO FUNDACIÓN SM, A.C.	México
PPC EDITORIAL, S.A. DE C.V.	México
SM DE EDICIONES, S.A. DE C.V.	México
ISME, LLC.	Puerto Rico
SM, INC.	Puerto Rico