Ithaka Group

Ithaka Infrastructure Partners SGEIC, S.L.

Internal Information System Policy

October 2025

1 Introduction

1.1 **Ithaka Infrastructure Partners SGEIC, S.L.** (hereinafter, "**Ithaka**"), in fulfilment of its commitment to applicable law and the highest ethical and professional standards, has drawn up and approved this Internal Information System Policy (hereinafter, the "**Policy**"), which shall also apply to its subsidiaries and funds (hereinafter, the "**Ithaka Group**").

1.2 Through this Policy, the Ithaka Group complies with the requirements arising from Law 2/2023, of 20 February, regulating the protection of persons who report regulatory regulatory breaches and the fight against corruption (hereinafter, "**Law 2/2023**"), adopted as a result of the transposition of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law.

2 Purpose

2.1 This Policy forms a core element of the Ithaka Group's Internal Information System and, together with the Information Management Procedure (hereinafter the "**Procedure**"), seeks to provide the Ithaka Group with the necessary resources and principles of action to encourage the use of the Whistleblowing Channel (hereinafter the "**Channel**"), and to ensure in this process the rights of all parties involved, particularly the guarantee of confidentiality, the prohibition of retaliation, the right of defence, the right to honour and the presumption of innocence.

3 Scope

3.1 This Policy applies to:

a) Members of the Board of Directors and management bodies of the Ithaka Group, including, where applicable, non-executive members, as well as all members of senior management .

b) Any employee of the Ithaka Group, including interns, trainees, as well as those whose employment relationship has not yet commenced when the information regarding breaches they intend to report was obtained during the selection process or pre-contractual negotiations.

c) Any person working for or under the supervision and direction of contractors, subcontractors and suppliers of the Ithaka Group.

d) Where applicable, the employees' legal representatives in the exercise of their duties to advise and support the whistleblower.

e) Individuals who, within the organisation where the whistleblower works, assist them in the process.

f) Individuals who are related to the whistleblower and who may suffer reprisals, such as the whistleblower's colleagues or family members.

g) Legal entities for which the whistleblower works or with which they have any other type of relationship in a work context, or in which they hold a significant stake (significant being understood as one that allows the person to exert influence over the legal entity).

4 Scope of protection

4.1 This Policy protects against any form of retaliation that may be directed at any natural or legal person who makes legitimate use of the Channel for the purpose of reporting any acts or omissions that may constitute a breach of:

- of European Union law,
- criminal offences or serious or very serious administrative offences, including – but not limited to – all infringements involving financial loss to the Treasury or the Social Security system, or relating to health and safety at work.

4.2 The protection afforded by this Policy and the other elements of the Internal Information System (hereinafter "**IIS**") shall not preclude the application of the rules relating to criminal proceedings, and is without prejudice to the provisions of labour legislation on health and safety at work for those who report breaches in this area.

5 Statement of Principles

5.1 The IIS shall be the preferred channel for reporting any breaches within its scope of application and shall be governed by the following operating and management principles:

1. Effectiveness and accessibility: the IIS must ensure that reports can be easily submitted, and that they are handled effectively, thereby enabling the organisation itself to be the first to become aware of any potential irregularities.
2. Independence: all persons involved in the management of the IIS must offer a guarantee of independence, in particular the IIS Responsible, so that any potential conflicts of interest or personal or professional ties that could affect the sound judgement or credibility of those involved in the communication management process are beyond reproach.
3. Confidentiality: the IIS shall be designed and managed in such a way as to guarantee the confidentiality or security of the identity of the whistleblower, the persons concerned and any third parties mentioned in the communications, as well as of the procedures carried out in the management and processing of such communications, so that this information is processed only by those persons competent and authorised to manage the IIS. The record of communications supervised by the IIS Manager shall be regulated in such a way as to guarantee not only the protection of personal data, but also the appropriate restriction of access to unauthorised personnel.
4. Presumption of innocence and right to honour: the persons concerned shall have the right to the presumption of innocence and the right of defence, such that under no circumstances may a presumption contrary to the person concerned be made when investigating or resolving a communication submitted.

   To this end, the persons concerned shall have the right to access the file in accordance with the terms set out in Law 2/2023, to receive the same protection as whistleblowers, and to be heard and to be able to submit representations in the internal investigation procedure whenever they deem it appropriate.
5. Prohibition of retaliation: retaliation against those who report or cooperate in a reporting or information-sharing process falling within the scope of protection of this Policy is expressly prohibited.

Retaliation shall be understood to mean any act or omission prohibited by law or which, directly or indirectly, constitutes unfavourable treatment that places the person suffering it at a particular disadvantage in the workplace or professional context solely because of their status as a whistleblower or their cooperation in the handling of information.

By way of example, the following conduct may be considered retaliation:

- Suspension of the employment contract, dismissal, termination of employment or non-renewal – unless this is carried out within the normal exercise of managerial authority in accordance with employment legislation.
- Damages, including reputational damage, financial loss, coercion, intimidation, harassment or ostracism.
- Negative references regarding professional work.
- Inclusion on blacklists or the dissemination of information within a sector that hinders access to or promotion within employment.
- Denial or cancellation of leave or training.

6. Principle of good faith: just as retaliation is prohibited, the Ithaka Group will not permit the use of the IIS for illegitimate, personal or bad-faith purposes.

   Should any whistleblower or third party involved misuse the IIS, such conduct may result in the Ithaka Group imposing the appropriate disciplinary sanction, where applicable, or taking any civil or criminal action that may be relevant.

6 IIS Responsible

6.1 In fulfilment of its obligations relating to the supervision and promotion of the IIS, the Board of Directors of Ithaka shall appoint the IIS Responsible.

6.2 The appointment and removal of the IIS Responsible shall be notified to the Independent Authority for Whistleblower Protection (A.A.I.) within ten (10) working days, specifying, in the event of removal, the reasons justifying such action.

6.3 The IIS Responsible shall perform their duties independently and autonomously from the other bodies of the Ithaka Group. Their duties include:

- Continuously promoting and supervising the implementation and effectiveness of this Policy.
- Ensuring access to this Policy for all members of the Ithaka Group and interested third parties.
- Implementing procedures to manage communications received through the Channel.
- Reviewing, investigating and issuing reports on any investigations arising from communications received through the Channel.
- Reporting the most significant results of the Channel's activity to the Ithaka Board of Directors as part of its reporting duties.

7 Publication of the channels

7.1 In accordance with the provisions of Law 2/2023, the Ithaka Group has published on its website, in a separate and easily accessible section, information regarding access to the Channel and this Policy.

7.2 The Ithaka Group undertakes to give this Policy and the Channel due publicity, providing all members of the Group and third parties linked to its professional activity with the necessary information and, where appropriate, training on the matter, to ensure free access to them and to all the IIS tools through which they may assert their legitimate rights.

7.3 Regardless of the access provided to this Ithaka Group Channel, any whistleblower may also approach the Independent Whistleblower Protection Authority.

8 Data protection

From the perspective of personal data protection, the main aspects applicable within the framework of the IIS are set out in Title VI of Law 2/2023 and are detailed below:

8.1 The processing of personal data arising from the application of Law 2/2023 shall be governed by the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR), in Organic Law 3/2018 of 5 December on the Protection of Personal Data and the Guarantee of Digital Rights (LOPD GDD), Organic Law 7/2021 of 26 May on the protection of personal data processed for the purposes of the prevention, detection, investigation and prosecution of criminal offences and the enforcement of criminal sanctions, and Title VI of Law 2/2023, as well as any other applicable legislation.

8.2 Personal data whose relevance to the processing of specific information is not apparent shall not be collected; if collected accidentally, it shall be deleted without undue delay.

8.3 The processing of personal data necessary for the application of Law 2/2023 shall be deemed lawful.

8.4 As Ithaka is an entity required to have an IIS, the processing of personal data, in cases of internal communication, shall be deemed lawful by virtue of the provisions of Article 6.1.c) of the GDPR – the processing is necessary for compliance with a legal obligation to which the controller is subject – and Article 11 of Organic Law 7/2021 of 26 May.

8.5 Where the processing of special categories of personal data is carried out for reasons of substantial public interest, it may be carried out in accordance with the provisions of Article 9.2.g) of the GDPR.

8.6 Where personal data is obtained directly from data subjects, they shall be provided with the information referred to in Article 13 of the GDPR and Article 11 of the LOPD-GDD, as set out in the privacy policy governing the IIS and the Channel.

8.7 Whistleblowers and those who make a public disclosure shall also be expressly informed that their identity will in all cases be kept confidential, and that it will not be disclosed to the persons to whom the reported facts relate, nor to unauthorised third parties or those linked to the management of the IIS.

8.8 The person to whom the reported facts relate shall under no circumstances be informed of the identity of the whistleblower or of the person who made the public disclosure.

8.9 Data subjects may exercise the rights referred to in Articles 15 to 22 of the GDPR.

8.10 Should the person to whom the facts described in the communication or to whom the public disclosure relates exercise their right to object, it shall be presumed, unless there is evidence to the contrary, that there are compelling legitimate grounds justifying the processing of their personal data.

8.11 The IIS will not obtain data that allows the whistleblower to be identified and will have adequate technical and organisational measures in place to protect the identity and ensure the confidentiality and security of

the data relating to the persons concerned and any third party mentioned in the information provided, particularly the identity of the whistleblower should they have been identified.

8.12 The identity of the whistleblower may only be disclosed to the judicial authority, the Public Prosecutor's Office or the competent administrative authority in the context of a criminal, disciplinary or sanctioning investigation.

8.13 The processing of data by other persons, or even its disclosure to third parties, shall be lawful where necessary for the adoption of corrective measures within the Ithaka Group or the handling of any relevant proceedings.

8.14 Access to personal data contained in the IIS shall be limited, within the scope of their powers and functions, exclusively to:

a) The IIS Responsible and those who manage it directly.
b) The head of human resources or the duly designated competent body, only where disciplinary measures may be taken against an employee. In the case of public sector employees, the competent body for handling the matter.
c) The head of the legal services of the entity or body, should legal action be required in relation to the facts set out in the report.
d) Any data processors who may be appointed.
e) The Data Protection Officer.

8.15 Similarly, where necessary for the purposes of the communication, personal data may be shared between the entities of the Group to which the data controller belongs, as well as with the relevant governing and representative bodies of the Ithaka Group and the Group entities involved.

8.16 The Data Protection Officer can be contacted via gdpr@ithaka.com