REPORTING, INVESTIGATIONS, AND ANTI-RETALIATION POLICY

May, 2025

Revision

Revision	Summary of Changes	Date
5	Added policy against attempts to unmask (identify) the individual who made a confidential report. Replaced usage of “Ethics and Compliance representative” with “Ethics representative” and “Ethics and Compliance Office” with “Ethics team” throughout.	1-May-25

History

Type of document	Governing	**Version**	5
Owner	Julianna Fox, Chief Ethics, Compliance and Sustainability Officer		
Approval		**Version**	**Approval date**
Policy Approval Committee		5	1-May-25
Governance, Ethics, and Compensation Committee (GECC)		5	1-May-25
Governance, Ethics, and Compensation Committee (GECC)		1	10-Aug-21
Governance, Ethics, and Compensation Committee (GECC)		2	25-Apr-22
Governance, Ethics, and Compensation Committee (GECC)		3	8-May-23
Governance, Ethics, and Compensation Committee (GECC)		4	25-Jul-24

Introductory statement

This **Reporting, Investigations, and Anti-Retaliation Policy** (the "**Policy**") supports WSP's commitment to putting ethics at the centre of all we do. WSP's commitment is notably reflected by the following actions.

1. We encourage a "Speak Up" culture by ensuring that internal reporting channels are effectively managed and communicated.
2. We protect against retaliation against any individuals who, in good faith, report misconduct, participates in, or collaborate with, an investigation.
3. We treat allegations of misconduct appropriately and carry out consistent, fair and effective internal investigations.

This Policy applies to WSP Global Inc. and its subsidiaries, and to all current and former employees, including directors, officers, trainees, apprentices, job applicants, and other persons subject to a current or former employment-type or work-related relationship with WSP, as well as independent contractors. Additionally, any third party may report potential breaches of WSP's Code of Conduct or of applicable laws and regulations pursuant to the terms of this Policy.

Duty to Report

Employees must report promptly any potential misconduct which could breach WSP's Code of Conduct, policies or applicable laws. Examples of misconduct include:

- Fraud, theft, improper accounting, money laundering or false claims,
- Corruption, conflicts of interest, kickbacks, and bribery,
- Unfair competition and insider trading,
- Actions that pose serious environmental risk,
- Actions that endanger health, safety, labour, or civil rights,
- Breach of data protection, confidentiality, privacy, or IT security,
- Violations of economic sanctions and trade controls,
- Improper interpersonal behavior such as violence, discrimination, harassment, and sexual harassment,
- Any form of retaliation against any person who reports potential misconduct or person who participated in an investigation,
- Any other conduct that could violate or encourage other employees to violate the law, our Code of Conduct, or policies.

When should I report?

Make your report as soon as potential misconduct is identified. You do not need to prove an allegation and should not conduct your own investigation before filing. This will be handled

by WSP's Ethics team or other team authorized to perform the relevant type of investigation. Do not delay reporting your concerns or attempt to take matters into your own hands: this can impede WSP's ability to effectively address the matter.

Can I report anonymously?

Yes, while we encourage reporters to identify themselves and participate in the investigation process, reporters can remain anonymous when filing a report through WSP's Business Conduct Hotline, operated by EthicsPoint, if permitted by applicable law to do so. All reports are reviewed promptly and addressed appropriately, according to the nature of the issues, regardless of whether or not the reporter chose to remain anonymous.

Where the identity of the reporter is known (or any other information from which their identity could be inferred), only those authorized individuals competent to receive, investigate or follow-up on reports shall have access to information with respect to their identity.

Other measures taken to keep reports and investigations confidential include access restricted record-keeping and limited distribution of investigation reports.

However, in certain circumstances, and as permitted by law, the identity of the reporter may be disclosed to other stakeholders.

What if I have a question or need advice regarding suspected misconduct?

If you are uncertain whether an incident or behaviour you observed or have become aware of a misconduct that should be reported, you are encouraged to first raise your concern on a confidential basis with your direct manager, the Ethics team or the other channels described below.

Reporting Channels

There are numerous reporting channels available to persons who wish to report potential misconduct, raise a concern, or ask a question. These reporting channels are established for the purpose of allowing employees and other stakeholders to report concerns and instances of potential misconduct.

While reporters may use any reporting channel available to them, employees are encouraged to first address any concerns they may have directly with WSP. In case of doubt, employees are always encouraged to report any concerns through the internal recipients listed below:

In Person

- Your People Manager,
- The Chief Ethics, Compliance and Sustainability Officer or an Ethics representative,
- A Human Resources representative,
- Where identified on the regional intranet, a Local Point of Contact duly appointed by the Ethics team to serve as confidential facilitator for reporters,
- The Global Vice President of Internal Audit or a member of the Internal Audit team.
- Regional HSE Leads/ Global VP HSEQ – Health, Safety, Environmental Concerns

Ethics Inbox

Concerns may also be reported directly to the Ethics team.

Email: ethics@wsp.com or alternate regional inbox managed by the Ethics team, as provided on the regional intranet

Mail: Ethics Team

1600 René Lévesque Blvd. West, 18th floor

Montreal, Quebec Canada H3H 1P9

Business Conduct Hotline

WSP has a Business Conduct Hotline or “whistleblowing hotline” operated by NAVEX EthicsPoint, an independent and secure reporting service. Concerns can be filed anonymously, both by telephone at the dedicated phone numbers identified on the Business Conduct hotline page, or by completing the online form here. The service is available in many languages, 24 hours a day, 365 days a year.

Local or National Reporting Options

Certain countries in which we operate may require that a local or national reporting option be available. Where applicable, the details and contact information for those local reporting channels, operated by the local Ethics team, will be provided on your local intranet. Reporters may, if they choose to do so, report to any such local reporting channel.

Employees may have more than one reporting option available to them, depending on their work situation and the laws applicable in the country or region in which they are located, in addition the channels established by WSP described above. For example, certain countries require that employees are made aware of relevant local bodies to which external whistleblowing reports may be made (which will be displayed on your regional intranet), or an employee may be embedded with a client who has its own reporting channels.

Health, Safety & Environmental Incidents

Health, Safety & Environmental incidents should be reported in accordance with the Global HSEQ Manual. In case of doubt, employees are nonetheless encouraged to report any concerns through the internal recipients listed above in section “3. Reporting Channels”.

Duties during an investigation

WSP will review all reports of potential misconduct for a response, referral or investigation. WSP will investigate allegations of potential misconduct in a consistent, fair and effective manner.

If the investigation reveals or substantiates misconduct, action will be taken, in accordance with internal procedures and applicable regional processes, to address the misconduct. Resulting actions may include remediation measures, such as policy updates, remedial training, communication campaigns, and disciplinary action, up to and including dismissal. Disciplinary action varies depending on the nature and severity of the misconduct, whether the misconduct is recurrent, as well as the requirements of applicable local law.

Employees must cooperate fully and in good faith with investigators who are performing internal investigations, including by attending meetings and providing information that the investigator requests and that they are legally permitted to share. Failure to cooperate may result in disciplinary measures. Participants should not expect to be given the full details of the allegations being investigated, as these are shared only on a need to know basis to preserve the integrity of the investigation.

What happens after I report?

All reports, regardless of the nature or the gravity of allegations they may contain, will be duly reviewed and processed by WSP in a consistent, fair and effective manner. Once a report is made, it will be acknowledged within 7 days. WSP’s objective is to close matters

within 60 days from the date on which the report was received. Not all reported concerns will necessarily result in an investigation.

How are investigations conducted?

An investigation may be initiated to determine if an allegation is well-founded. The reporter will receive information about the outcome or progress of a review as soon as reasonably possible and/or within legal timeframes. An investigation is not a disciplinary or punitive process, though it may result in disciplinary action in certain cases, such as when misconduct has been substantiated.

What about the confidentiality of the investigation?

Reports and information gathered during an investigation are treated as confidential. Appropriate treatment by the investigators drives WSP's ability to maintain its Speak Up culture and preserves the integrity of the investigation process. Such information will be handled in accordance with our Global Information Security Policy and revealed only as necessary for the purpose of answering the question(s) raised by the report, or to allow WSP to fulfill its legal obligations or legitimate business needs. Further information about the management of personal data can be found in the Privacy Policy.

Prohibition on retaliation

Retaliation occurs when adverse action is taken against a person in response to them having reported misconduct, participated in an investigation, refused to participate in suspected improper activity or exercised workplace rights protected by law.

WSP has a zero-tolerance policy against any form of retaliation and is committed to a workplace culture where employees feel safe to raise concerns at any time without fear of adverse consequences. Employees must not retaliate against anyone who filed a report in good faith or participated in an investigation. In addition, employees may not attempt to learn the identity of a reporter.

WSP's anti-retaliation protection extends to employees, third party reporters, witnesses, persons who assisted the reporter in the investigations process, persons connected with the reporter who could suffer retaliation, or legal entities owned by the reporter. Acts, threats or attempts of retaliation are a serious violation of the Code and will be investigated. Anyone found to have engaged in retaliation will be subject to disciplinary action, up to and including dismissal.

What are examples of retaliation?

Retaliation refers to any form of adverse action, direct or indirect, taken against a person for reporting misconduct or otherwise exercising their rights protected by law. Retaliation can take many forms, including:

- Demotion;
- Suspension;
- Dismissal;
- Salary reductions,
- Job reassignments, including transfer of duties, change of location of place of work, reduction in wages, change in working hours,
- Failing to promote, including failure to convert a temporary employment contract into a permanent one, where the worker had such legitimate expectations,
- Creating a hostile work environment, including coercion, intimidation, harassment or ostracism,
- Adversely impacting working conditions,
- Withholding of training,
- Imposition of any disciplinary measures, reprimands or other penalties, including financial penalties,
- Causing reputational harm, particularly in social media, or financial loss,
- Denying employment benefits.

What should I do if I fear retaliation?

WSP is fully committed to protect all persons who file a report or cooperate in an investigation from any form of retaliation. If you are concerned, include a note in your report or directly notify the investigator, ethics@wsp.com or an Ethics representative.

What should I do if I believe someone is experiencing retaliation?

If you observe or suspect an act of retaliation, you must report the concern immediately through one of the available reporting channels described in the “Reporting Channels” section above or directly notify the investigator, ethics@wsp.com or an Ethics representative.

Regional implementation

This policy applies to all WSP operating entities, who ensure that its adoption is in compliance with all applicable legislation. Accordingly, WSP will issue a regional addendum to this policy, where required, which will apply to reports made in that particular country. Where there is a discrepancy between this Policy and local law, WSP will apply the stricter requirements.

Information management and document retention

Regardless of the reporting channel used, the collection and processing of personal data as part of a report and subsequent investigation will be processed in accordance with our WSP Privacy Notice. A dedicated Online Reporting Privacy Notice is available before submitting a report.

WSP employees may, as part of their work duties, come in contact with information or documents that are controlled, restricted, or otherwise confidential. This includes, for example, information about defense contracts, export-controlled data, military-use technology or other sensitive or classified information. This type of controlled information must not be included in an incident reported under this Policy.

WSP will keep records of every report received, in compliance with the confidentiality requirements provided for in our Global Information Security Policy. Reports shall be stored for no longer than it is necessary and proportionate, in compliance with WSP's records management practices, in order to comply with the requirements imposed by applicable law.

Related documents

- Code of Conduct
- Global Delegation of Authority
- WSP - Online Reporting Platform Privacy Notice
- Global Privacy Policy
- Information Classification and Handling Policy
- Records Management Policy
- HSEQ Manual

Where to turn for help

If in doubt about any aspect of this Policy, employees may visit the Global Investigations page on WSP's intranet for more information, contact ethics@wsp.com or communicate directly with their regional Ethics representative. Their contact information is available on WSP's intranet site.