Group Speak Up & Investigations Policy

Document reference: GABCF:01
Issue: **3.0**

[X] UK [X] USA
[X] Canada [X] Australia

Owner: **Mia Wellfare**
Date: September 2025

Amendment record sheet

Issue	Summary description of change
1	Initial release – October 2023
2	Update – November 2024 Addition of Compliance Champions to document Addition of SpeakUp hotline for reporting concerns of retaliation
3	Review in line with introduction of ECCTA 2025

CONTENTS

Section 1. OVERVIEW

To report a concern, please access the Speak Up Hotline online via https://speakup.ultra.group or via the phone number for your location, listed below in Section 2.2. For any questions on reporting or this Policy, please contact our Chief Compliance Officer Mia Wellfare at Mia.wellfare@ultra-electronics.com.

1.1. Introduction

Ultra Electronics Holdings Ltd ('Ultra' or 'our') and each of its respective business units is committed to conducting business with honesty and integrity, and Ultra expects all our colleagues, partners, contractors, and vendors to maintain the highest ethical standards and always operate in accordance with Ultra's Code of Conduct.

The aim of this Speak Up and Investigations Policy ('Policy') is to encourage you to raise any genuine concerns you might have about suspected wrongdoing within or in connection with Ultra without fear of reprisal. The Policy explains how such concerns can be raised within Ultra, and how they will be appropriately investigated.

1.2. Eligibility

The Policy applies to all individuals working for or with Ultra, at all levels and grades, including senior managers, officers, directors, employees (whether permanent, fixed-term or temporary), consultants, contractors, trainees, seconded staff, home workers, casual workers and agency staff, volunteers, interns, agents, sponsors, or any other person associated with us, or any Ultra subsidiaries or their employees, wherever located (collectively referred to as 'Workers').

1.3. Obligation to Speak Up

Doing the right thing and speaking up can be hard sometimes. It is important to report any concern you have, even if you are not 100% sure there is a violation. This is so the matter can be investigated and, if any wrongdoing is found, can be stopped immediately. This obligation is not simply encouraged; it is required. If you are uncertain whether something is within the scope of this Policy, you should seek advice from a Compliance Champion, your Manager or Human Resources.

Speaking up about potential concerns is the right thing to do — and anyone who raises a concern in good faith will never be penalised for doing so. Reporting concerns gives Ultra the opportunity to investigate and address any potential issues; it also helps us maintain a positive, open working environment.

Any concerns that fall within the scope of this Policy should be raised pursuant to this Policy and internally within Ultra. You should not bypass this procedure and raise your concerns externally on any Social media or review sites - such as YouTube, Twitter, Facebook, Indeed or Glassdoor - are public spaces that are not an appropriate channel for raising concerns**.**

Section 2. HOW TO SPEAK UP

2.1. Direct Reporting

It is important to identify and escalate potential issues as early as possible. Ultra therefore encourages you to report concerns to anyone listed below. Reports to the following people can be made through any medium, including in-person, by telephone, and by email.

You can raise concerns to any of the following:

- Direct and indirect supervisors;
- Human Resources;
- Ultra Group or Business Unit Legal;
- Ultra Group Compliance or Local Compliance Champion; or
- Senior Management.

The person to whom any report is made will record the report into a central case management system, which Ultra Security, Legal or Compliance teams will promptly assess to determine next steps, while maintaining confidentiality.

2.2. Speak Up Hotline

Should you feel that you are unable to report a potential issue to one or more of the people listed above, Ultra also has an independent, anonymous, and confidential EthicsPoint hotline ('Speak Up Hotline') to facilitate and encourage employees to raise concerns. You can report directly to the Speak Up Hotline available 24 hours a day, 7 days a week, which is administered by Navex Global. This service maintains a central case management platform, which Ultra Security, Legal or Compliance teams will promptly assess to determine next steps.

You may access the Speak Up Hotline via:

- Online at https://speakup.ultra.group
- Phone:
  - Australia: 1800-953607
  - Canada: 1-866-225-1317
  - United Kingdom: 0808-238-7511
  - United States: 1-866-225-1317

US employees in our mitigated businesses, please note Speak Up is not the appropriate place to register a security violation. Those reports should be made to your Facility Security Officer ('FSO') or the Department of Defense Hotline according to the requirements of the National Industrial Security Program Operating Manual.

If you are in a company that operates under the Special Security Agreement ('SSA') and wish to raise concern about a matter that may involve classified information, you should not include that classified information in your initial report. Contact your FSO in the first instance if you are not sure who can give you advice on what you can and can't say. If you are in the UK, Canada or Australia and your report contains classified information speak to your local security officer in the first instance.

2.3. What Should Be Reported

Workers ***must*** report any actual or suspected violations of laws; regulations; and Ultra standards, policies, and procedures. This includes, but is not limited to potential:

- criminal offences, including corruption, bribery, and fraud;
- failures to comply with any legal obligations or regulatory requirements;
- dangers to the health and safety of any individual;
- fraud or mismanagement of company finances or other assets including company information;
- breach of Ultra policies or procedures, including the Code of Conduct;
- tax evasion;
- unauthorised breaches of confidential information or privilege;
- serious negligence that could or does result in unacceptable loss, damage or injury.

- conflicts of interest;
- data breaches;
- discrimination and harassment;
- environmental, social, or governance concerns;
- unfair competition;
- other conduct likely to damage Ultra's reputation or financial position; or
- the deliberate concealment of information concerning any of the matters listed above.

2.4. What to Include

To help Ultra address your concerns, please provide as many facts and details as you can. Specifically, please provide:

- the business and location the report is referring to;
- the background, history, and reason for the concern;
- dates, places, and if possible, names of those involved;
- any documents that may be helpful; and
- any discussions you have had about your concerns with others.

You may always make reports anonymously (without identifying yourself), but identifying yourself will likely result in a more efficient and thorough investigation. Should you raise your report via Speak Up, you will receive a report key and password to follow up on your submission. Please login approximately 5-6 working days after completing the online report to see if any queries have been raised for your comment. Please respond to these promptly.

Section 3. PROTECTION AND ANTI-RETALIATION

Ultra is committed to ensuring that all good faith reporters are treated with respect and protected from harm, including retaliation, dismissal, demotion, or other harm or threats.

3.1. Confidentiality

Ultra aims to deal with allegations raised under this policy sensitively and with due respect for the privacy of the individuals involved. All employees must treat as confidential any information communicated to them in connection with an allegation made under this Policy. Subject to applicable law, Ultra will disclose reports only to individuals necessary to ensure proper review and resolution. If you identify yourself in the report, Ultra will take all possible steps to protect your identity. Please be reassured that Ultra will not tolerate any retaliation against you if you do choose to disclose your identity.

3.2. Data Protection and Record Keeping

Conducting investigations and hearings under this policy may involve processing personal data of the employees concerned. Ultra uses personal data to investigate and deal with whistleblowing allegations.

Ultra will keep records of complaints dealt with under this procedure during employment and in accordance with the relevant data retention policy after employment ends. More general information, including details of who your personal data is shared with, your rights under data protection law and who you should contact if you have any concerns is available from your local HR team.

3.3. Non-Retaliation

Anyone who seeks advice or raises a concern in good faith — whether directly to a manager, another person at the Company, or through the Speak Up Hotline — is doing the right thing and will be protected from retaliation. Ultra does not allow retaliation of any kind, no matter what happens with the issue raised. Retaliation is a violation of this Policy, and may result in disciplinary action, including termination.

Ultra may take appropriate action against any person found to be:

- victimising another person for using this Policy; or
- deterring any person from reporting genuine concerns under this Policy.

Please tell your Manager, HR Director, Local Compliance Champion or the Chief Compliance Officer if you think you have been victimised or deterred, and / or report the concern via Ultra's Speak Up Hotline.

Section 4. What Happens Next: Investigation Procedure

Ultra takes all good faith reports seriously. All reports will be first reviewed by US Security personnel to ensure no DoD restricted information has been provided. Once security is cleared, the report will be reviewed by Ultra Chief Compliance Officer or his or her designee (the 'Screener') to determine appropriate next steps, which may include an investigation. Every investigation will be conducted objectively, confidentially, and accordance with this Policy.

The Chief Compliance Officer must recuse herself or himself from any reports and investigations involving allegations concerning or relating to the Chief Compliance Officer, or any other situation that presents an actual or perceived conflict of interest.[1] In such a case, the Chief Compliance Officer must disclose the recusal to the Ultra Board of Directors, which must then make (or appoint an appropriate Screener to undertake) the initial assessment outlined below in Section 4.1.

4.1. Initial Assessment

Upon receiving a report of suspected or actual wrongdoing, the Screener will review the report and make an initial determination to assess: (1) the nature of the report (e.g., workplace safety, bribery, employment dispute); (2) the initial creditability of the report (i.e., whether the report was made in good faith); and (3) what additional information would be necessary to substantiate the report. The Screener's initial assessment will not be coloured by the identity of the reporter, or the identity of the person who is the subject of the report (if known).

If the Screener determines that additional information is necessary to complete the initial assessment, the Screener will attempt to contact the reporter for further information. Upon receiving the initial assessment, the Chief Compliance Officer (or his or her designee) will determine (1) whether the matter requires additional investigation; (2) what the appropriate next steps are; and (3) who will be responsible for managing the next steps.

[1] Note: the CMS automatically blocks an employee from accessing a report in which they are named or referenced.

The Chief Compliance Officer may, at his or her reasonable discretion, (1) investigate the report herself or himself; (2) authorise another Ultra employee to investigate the report, (3) engage outside counsel to investigate the report; or (4) close the report. The Chief Compliance Officer may only close a report during the Initial Assessment if they make a reasonable determination that the report was not filed in good faith or is otherwise not credible, a note of any such decision will be made in the EthicsPoint case management system ('CMS'). Any communications with legal counsel will be protected under attorney-client privilege and should not be disclosed to third parties.

The Chief Compliance Officer may not authorise any Ultra employee to investigate the report who has an actual or potential conflict of interest with the reporter and/or the subject of the report.[2]

4.2. Conducting Investigations

Ultra will take a risk-based approach to scoping and conducting investigations of potential wrongdoing. This means that the scope of Ultra's investigation will turn on the nature and substance of the report.

Ultra's investigation can include, but is not limited to, conducting interviews with witnesses, analysing books and records, and reviewing email and other communications, documents, and materials. This may include requesting additional information from the reporter.

Ultra will aim to keep any good faith reporters generally aware of the timeline of the investigation, to the extent that it is known, but it cannot share details of the status of the investigation with anyone. Any investigations will be conducted confidentiality in order to protect the integrity of the investigation. Ultra documents the status of the investigation in its CMS. Any investigations that are subject to the attorney-client privilege or attorney work product privilege will be referenced in the CMS as such, and in order to preserve privilege over the investigation, will not include any detailed information that could constitute a waiver of such privilege. Communications concerning potentially privileged investigations will be limited to senior Ultra leadership and counsel.

4.3. Resolution

Ultra strives to resolve every report, and aims to do so in a timely and efficient manner.[3] Once an investigation has concluded, the Chief Compliance Officer, or his or her

[2] Note: the CMS automatically blocks an employee from accessing a report in which they are named or referenced.

[3] Ultra aims to respond to a reporter's initial Speak Up within 48 hours, and complete investigations within 90 days. For more complex or serious matters these timeframes may be adjusted to ensure a comprehensive investigation of issues.

designee (the ‘Remediator’), and when they deem necessary, in consultation with the relevant Investigation Disciplinary Committee (‘IDC’) and / or Board of Directors, will determine whether the investigation found the report: (1) substantiated, (2) partially substantiated, (3) undetermined, or (4) unfounded.

The Remediator, in consultation with any formed IDC and / or Board of Directors, shall determine and implement any appropriate remedial steps following the conclusion of an investigation. This can include but is not limited to: (1) employee discipline (including termination); (2) compliance control enhancements; (3) compliance training measures, and (4) referrals to law enforcement.

If appropriate, Ultra will notify the reporter of the outcome (un/substantiated) once the investigation has concluded and consider other relevant notifications it is required to make.

Section 5. Document Information

5.1. Status of This Policy and Procedure

This Policy does not give contractual rights to any individual. The company reserves the right to alter any of its terms at any time although Ultra will notify you in writing of any changes**.**

5.2. Related Documents

For further guidance regarding Ultra’s commitment to a culture of compliance, please refer to the following Group and related Local policies:

- Code of Conduct
- Anti-Bribery, Corruption and Fraud Manual
- Gifts and Hospitality Procedure
- The Selection and Management of Intermediaries Procedure
- Anti-trust and Competition Law Policy
- Health and Safety Policy

5.3. Document Ownership and Review

This Policy has been produced for use within the Ultra Electronics Group.

The Company reserves the right to change, amend, or review this policy and procedure as required from time to time at its discretion. At a minimum it will be reviewed annually.

For questions or more information about this Policy, please contact Mia Wellfare at Mia.wellfare@ultra-electronics.com