WHISTLEBLOWER POLICY

1. Introduction

Ultradata is committed to the highest standards of conduct and ethical behaviour in all of our business activities and to promoting and supporting corporate compliance and honest and ethical behaviour. Behaving ethically and in compliance with our obligations is also good for Ultradata's business.

We are committed to creating a culture where those involved with our organisation feel safe to report improper conduct relating to the Ultradata Group, its officers and employees. This Whistleblower Policy is intended to protect whistleblowers and thus encourage reporting of improper conduct.

2. Purpose of this whistleblower policy

The purpose of this policy is to enable eligible people to report instances of suspected improper conduct involving the Ultradata Group by providing a convenient and safe reporting mechanism so that those who make a report may do so confidentially without fear of victimisation, harassment or discriminatory treatment.

The Policy aims to achieve this purpose by setting out:

- who can make a protected disclosure,
- what sort of conduct can be reported as a protected disclosure,
- who to make a disclosure to,
- how to make a disclosure,
- how people making disclosures are protected,
- how people making disclosures are supported,
- how investigations into a disclosure will proceed,
- how Ultradata will ensure fair treatment of employees who are mentioned in disclosures, and
- how Ultradata will make the policy available.

3. Who can make a protected disclosure?

This Policy applies to all Ultradata Group companies (collectively referred to as Ultradata). It applies to all directors and personnel including managers, employees, and contractors and also to clients and suppliers. "Disclosers" means anyone who is, or has been, in any of the following relationships with any entity within the Ultradata Group:

- employee;
- director;
- officer;
- contractor (including employees of contractors);
- associate;
- consultant; and
- relatives, dependants, spouses, or dependents or a spouse of any of the above.

The protections in this Policy will also apply to anyone who has made a disclosure of information relating to an entity in Ultradata to a legal practitioner for the purpose of obtaining legal advice or legal representation in relation to whistleblowing protection laws.

4. What sort of conduct can be reported as a protected disclosure?

4.1. What conduct is Reportable Conduct?

The protections in this whistleblower policy apply when people disclose "Reportable Conduct". The protections apply even if the disclosure turns out not to be correct. Disclosures that are not about Reportable Conduct do not qualify for protection under the Whistleblower Policy.

Reportable Conduct is defined to be "misconduct", "improper affairs", contravention of various legislation, and conduct posing a danger to the public or the financial system. Reportable Conduct covers a broad range of conduct, from a breach of Ultradata's Code of Conduct (which may not be a breach of any law) through to serious breaches of the law (for example, breaches of criminal offences such as fraud and theft, and ongoing conduct such as tax evasion or money laundering).

The following list gives some examples of Reportable Conduct, although it is not exhaustive.

Examples of Reportable Conduct:

- lying to or misleading clients
- falsifying invoices from suppliers, or claiming reimbursement of expenses not actually incurred
- paying a bribe to the purchasing officer of a client, or being paid a bribe from a supplier
- breaching compliance obligations such as data protection or anti-money laundering obligations
- theft of property from Ultradata or from a client
- harassment or intimidation of Ultradata staff or client staff (other than personal work related grievances, see below)
- financial irregularities in accounting systems
- negligence by Ultradata people, or that is done to Ultradata
- safety risks to people, including the public or the environment
- safety risks to systems, including the financial system.

4.2. What is not Reportable Conduct?

Not all conduct will fall within the definition of Reportable Conduct, even though that conduct could be considered wrong or improper. If the conduct is not Reportable Conduct then the Whistleblower Protections do not apply.

4.3. Personal work related grievances

Personal work related grievances are excluded from this Policy and the whistleblower protections and should be reported to your line manager or Human Resources representative in accordance with the Complaint Resolution/Grievance handling Policy at http://home/html/admin/procedures/complaint_resolution_procedure.html

"Personal workplace grievances" means a grievance solely about any matter in relation to the Discloser's employment, or former employment, having (or tending to have) implications for the discloser personally. This includes:

- interpersonal conflict between the discloser and another employee;
- decisions to discipline the discloser;
- decisions relating to the engagement, transfer or promotion of the discloser;
- decisions relating to the terms and conditions of engagement of the discloser;
- a decision to suspend or terminate the engagement of the discloser,

where the matter does not have significant implications for Ultradata or relate to Reportable Conduct.

A personal work related grievance may still be protected under this Policy if:

- It includes information about Reportable Conduct,
- Ultradata has:
  - Breached employment laws or other laws in ways punishable by 12 months or more imprisonment
  - Engaged in conduct that is a danger to the public,
- Threats of detriment are made to the discloser,
- The discloser is seeking legal advice about the operation of whistleblower laws.

4.4. Disagreement with a management decision

Just because a person disagrees with a business or management decision does not of itself make the decision Reportable Conduct.

A person who has a complaint about business decisions such as service levels, or management decisions such as policy directions, should speak to their contact manager at Ultradata about these issues.

If a person makes a disclosure and it is not about something that is Reportable Conduct then the protections that apply to whistleblowers do not apply.

4.5. Reasonable Grounds to Suspect Reportable Conduct

The protections in this Whistleblower Policy apply when people have 'reasonable grounds to suspect' Reportable Conduct. This means that there should be some information that when viewed objectively supports the suspicion. The Reportable Conduct does not have to be proven by the person making the disclosure. A mere allegation with no supporting information is not likely to be considered as having reasonable grounds to suspect Reportable Conduct.

5. Who to make a disclosure to?

5.1. Who can receive disclosures?

Disclosures can be made to a person or organisation who is authorised to receive the disclosure. Receivers are eligible recipients (Ultradata's authorised whistleblower protection officers, senior managers, directors, and auditors), and regulators (including ASIC, and APRA).

In certain circumstances, disclosures can be made to other people or organisations. See below for more information about when such disclosures are protected, see paragraphs 5.5 to 5.8 below.

If you need more information before formally making a disclosure, you can contact an authorised whistleblower protection officer.

Ultradata encourages people to disclose to a whistleblower protection officer at Ultradata so that Ultradata can address any issues as quickly as possible.

Whistleblower disclosures can be sent by email to values@ultradata.com.au or by post to Ultradata Values, CONFIDENTIAL, C/o Ultradata, PO Box 123 Darling, Victoria 3145 or to an authorised whistleblower protection officer listed below.

5.2. Whistleblower Protection Officers (WPOs)

NAME AND TITLE	*POST*
Chief Operating Officer	*Chief Operating Officer* *CONFIDENTIAL* *C/o Ultradata* *PO Box 123* *Darling* *Victoria 3145*
Chief Risk Officer	*Chief Risk Officer* *CONFIDENTIAL* *C/o Ultradata* *PO Box 123* *Darling* *Victoria 3145*
Chief Executive Officer	*Chief Executive Officer* *CONFIDENTIAL* *C/o Ultradata* *PO Box 123* *Darling* *Victoria 3145*
Chair	*Chair* *CONFIDENTIAL* *C/o Ultradata* *PO Box 123* *Darling* *Victoria 3145*

5.3. Senior Officers of Ultradata

You may also disclose the matter to a person in one of the following roles at Ultradata:

- a director in the Ultradata Group
- a senior manager in the Ultradata Group
- an auditor of Ultradata Group

- an actuary of the Ultradata Group.

5.4. Legal practitioners for the purposes of obtaining legal assistance about the whistleblower legislation

Disclosure to a legal practitioner for the purpose of obtaining legal advice about the operation of the whistleblower protection legislation are protected disclosures, regardless of the conclusions of the legal practitioner about whether or how the protections apply.

5.5. Regulators including ASIC and APRA

Disclosure can be made to a regulator specified in the legislation. The legislation currently prescribes ASIC and APRA as regulators to whom disclosures can be made. You can find more information about disclosing to ASIC at https://asic.gov.au/about-asic/asic-investigations-and-enforcement/whistleblowing/how-asic-handles-whistleblower-reports/

You can find more information about disclosing to APRA at https://www.apra.gov.au/become-a-whistleblower-and-make-a-public-interest-disclosure

5.6. Public interest and emergency disclosures

In certain circumstances a disclosure made to a parliamentarian or a journalist will be a protected disclosure. To be a protected disclosure to a parliamentarian or a journalist the disclosure must fall within the definition of 'public interest disclosure' or 'emergency disclosure'.

Please consider the requirements for protection, including that disclosure has previously been made to a regulator (ASIC or APRA), and other requirements noted below are satisfied. It is recommended that you seek legal advice before making a public interest or emergency disclosure.

5.7. Public interest disclosures

Public interest disclosures to a journalist or parliamentarian will be protected disclosures if:

- A disclosure has been made to a regulator, such as ASIC, APRA, or prescribed Commonwealth body at least 90 days previously, and
- The disclosure does not have reasonable grounds to believe action has been taken, and
- The discloser has reasonable grounds to believe making a further disclosure is in the public interest, and
- The disclosure has first written to the relevant regulator that the original disclosure was made to and stated that they intend to make a public disclosure. The discloser must provide the regulator with enough information to identify their previous disclosure.

5.8. Emergency disclosures

Public interest disclosures to a journalist or parliamentarian will be protected disclosures if:

- A disclosure has been made to a regulator, such as ASIC, APRA, or prescribed Commonwealth body, and

- The disclosure has reasonable grounds to believe the information concerns a substantial, imminent danger to health, safety or the natural environment, and
- The disclosure has first written to the relevant regulator that the original disclosure was made to and stated that they intend to make an emergency disclosure, and
- The extent of the information disclosed is no greater than necessary to inform the journalist or parliamentarian of the substantial and imminent danger.

6. How to make a disclosure

6.1. Make the disclosure to an authorised person or organisation

The protections in this Whistleblower Policy apply when people disclose Reportable Conduct to the people and bodies authorised to receive disclosures as set out in section 5 above.

6.2. Anonymous Reporting

Anonymous reports of wrongdoing are accepted under this policy and are protected disclosures if they comply with the requirements. Reports can be made anonymously, for example by sending written reports without your name directly to a WPO in paragraph 5.2 by mail or to the email address in paragraph 5.1. The discloser may also use a pseudonym, and does not have to answer questions that might reveal their identity in follow up communications.

Anonymous reports may hinder an inquiry or investigation by, for example, by preventing the gathering of further information to assist the inquiry/investigation. Maintaining anonymous two way communication after the disclosure by using an anonymous hotline phone number or an anonymous email address will allow the discloser to and recipient to ask follow up questions.

Anonymous reports may limit the ability to provide feedback on the outcome or provide feedback.

6.3. What to include in your disclosure

We encourage you to provide as much information as you can so that your report can be properly and quickly looked into.

7. How people making disclosures are protected

7.1. Protection of people making disclosures

Ultradata is committed to ensuring whistleblowers by protecting people who make qualifying disclosures. This is done through a combination of protections, as set out below. These protections apply whether the qualifying disclosure is internal or external.

7.2. Identity protection (confidentiality)

Ultradata has a legal obligation to protect a discloser's identity. A person cannot disclose the identity of a discloser (or information likely to identify the discloser) and doing so is illegal, except if the disclosure is:

- To ASIC, APRA, or the Federal Police, or another body prescribed by the law,
- Allowed or required by law,

- To a legal practitioner in order to obtain legal advice about the whistleblower protections, or
- With the discloser's consent.

The information provided by the discloser may be disclosed if:

- It does not include the discloser's identity,
- All reasonable steps are taken to reduce the risk the discloser can be identified from the information, and
- It is reasonably necessary to investigate the issues raised by the disclosure.

Disclosures that involve a threat to life or property, illegal activities or legal action against Ultradata may require actions that do not allow for complete anonymity.

Any breach of confidentiality in relation to the disclosure or whistleblower's identity will be taken seriously, and may be the subject of a separate investigation and/or disciplinary action. Complaints can be made to an Ultradata whistleblower protection office (see clause 5.2 or the Ultradata general whistleblower report email in paragraph 5.1) or to ASIC or APRA (see clause 5.5).

7.3. Protection from detrimental acts or omissions

Whistleblowers who make disclosures under this policy must not be personally disadvantaged by dismissal, demotion, harassment, discrimination, disciplinary action, bias or other unfavourable treatment connected with making a report including damaging the discloser's reputation or business or financial position. A person must not make a threat, whether express or implied, to disadvantage the discloser in anyway.

Managing unsatisfactory contract performance in line with Ultradata's management framework is not a detrimental act or omission.

7.4. Compensation and other remedies

If Ultradata fails to take reasonable precautions and due diligence to prevent detrimental conduct and the discloser suffers loss, damage or injury then the discloser can seek compensation and other remedies through the courts.

It is recommended that a discloser seeks legal advice about their rights to compensation and remedies.

7.5. Protection from civil, criminal and administrative liability

A discloser is protected in relation to their qualifying disclosure from:

- civil liability (breach of contract or confidentiality obligations),
- criminal liability (for unlawful disclosure or other prosecution) (but no protection for making a false disclosure, and
- administrative liability.

A discloser is not protected from civil or criminal liability for any of his or her conduct which may be revealed by the disclosure. However, if a discloser reports such conduct and actively co-operates in an investigation in which they may be implicated, there may be some cases where the fact they have made a report will be taken into account as a mitigating factor when determining actions which may be taken against them.

7.6. The practical steps Ultradata will take to protect the whistleblower's confidentiality

Ultradata will take steps to protect the whistleblower's identity, including:

- Redacting the discloser's personal information from reports and statements
- Using gender-neutral language when referring to the discloser
- Working with the discloser to remove aspects of their disclosure that may inadvertently identify them (where possible)
- Using qualified people to handle and investigate disclosures
- Storing material related to disclosures securely
- Limiting knowledge of the discloser's identity to direct investigators
- Limiting access to disclosed information to those directly involved in managing and investigating the disclosure
- Not using email addresses or printers or filing locations that can be accessed by other staff
- Reminding people involved in handling and investigating disclosures of the confidentially requirements and penalties for breach.

7.7. The practical steps Ultradata will take to protect the whistleblower from detrimental acts or omissions

Ultradata will take steps to protect the whistleblower from detriment, including:

- Assess the risk of detriment in response to a disclosure (to the discloser and to others suspected of disclosing)
- Take appropriate steps to protect the disclose from detriment, for example, allow the discloser to work from another place, or in another role, or reassign or relocate other staff
- Train management about their responsibilities to maintain confidentiality, to address risks of harassment or conflict, and ensure fairness in performance or management action relating to a discloser
- Providing information about how to complain about detrimental treatment or harassment.

8. How people making disclosures are supported

Ultradata will support people making disclosures by:

- Redacting the personal information of disclosers and witnesses from document,
- Ensuring records will be kept secure,
- Providing for confidential communications with the discloser and how this will be managed
- Assessing the risks of detriment to a discloser
- Providing support services
- Having procedures for a discloser to make a complaint about detriment they have suffered.

9. How investigations into a disclosure will proceed

Ultradata will:

- Assess the disclosure to determine whether it qualifies for protection
- Assess whether a formal, in depth investigation is required
- Appoint an appropriate investigator considering conflicts, independence, and expertise in the subject matter of the disclosure
- Ensure the time and place and method for making the disclosure and any follow ups are suitable and protect the discloser including requirements for anonymous communication
- Treat the disclosure confidentially
- Focus on the substance of the disclosure rather than any personal aspects
- Provide a guide to the keys steps in responding to the disclosure, subject to limits on anonymous communications.

10. How Ultradata will ensure fair treatment of people who are mentioned in disclosures

Ultradata will ensure fair treatment of individuals who are mentioned in disclosures by:

- handle disclosures confidentially (provided it is practical and appropriate to do so)
- ensure all investigations and assessments are objective, fair and independent
- inform the individual at an appropriate time in the investigation
- give the individual procedural fairness and apply the principles of natural justice before making any adverse finding against the person.

11. How Ultradata will make this Whistleblower Policy available

The Whistleblower Policy will be published on the staff intranet and a version will be published on the Ultradata public website.

Training will be provided to staff when the Whistleblower Policy is introduced and then on an ongoing basis. Separate training will be provided to Whistleblower Protection Officers.