ULTRA Intelligence & Communications

Corporate Global Policy Summaries

Anti-Bribery and Corruption

Ultra Intelligence & Communications (Ultra I&C) takes a zero tolerance approach to bribery and corruption and prohibits its employees from offering, giving, or receiving bribes or personal inducements, or requesting others to do so on their behalf, for any purpose. Any employee who breaches this policy may be subject to criminal prosecution and will face disciplinary action, which could result in dismissal for gross misconduct.

Bid Management Policy

Approval of Bids represents a key part of Ultra I&C's internal control system. It is important that Bids are competitive, present acceptable levels of risk and predict satisfactory financial returns. Compliance with this Policy ensures:

- bid prices are competitive and satisfactory levels of profitability are achieved
- risks are identified, evaluated and mitigated
- issues pertinent to the Bid are raised and addressed during the Bid approval process with adequate levels of internal scrutiny
- commercial, financial and legal obligations are managed appropriately

Communications Policy

Ultra I&C communicates in a variety of ways to various stakeholders including customers, suppliers, financial institutions and the general public. The Communication Policy helps protect Ultra I&C's reputation through consistent communications.

Competition Compliance Policy

Ultra I&C businesses must comply with local competition laws. Failure to comply with such laws can lead to significant fines based on worldwide annual turnover.

Contract Management Policy

Approval of contracts, contract changes and ongoing contract compliance management represents a key part of Ultra I&C's internal control system.

All Contracts entered into by the Ultra I&C businesses must be effectively managed from a financial, operational, technical, commercial and legal perspective throughout the Project lifecycle (negotiation, delivery, termination and expiration) to help realise financial objectives and mitigate and control contractual risk.

Compliance with this policy is required ensure:

- contracts and contract changes are properly negotiated and have a risk profile acceptable to the individual Ultra business.
- contract risks are identified, mitigated and managed.contract performance and compliance is reviewed throughout the Project lifecycle.
- contract change control processes are adopted and followed.

Corporate Environmental Policy

Ultra Intelligence & Communications conducts its activities in a responsible manner, having regard to their effect on the environment and the communities in which Ultra I&C operates.

Businesses are required to carry out their duties in such a way as to minimise environmental damage and maximise conservation of materials and energy in compliance with national, regional and local environmental legislation.

Data Protection Policy

Ultra I&C is committed to safeguarding the personal data of all data subjects. Known as Personally Identifiable Information in some of the countries where Ultra I&C operates, personal data is only ever processed where there is legitimate and lawful reason to do so. Where explicit consent is required Ultra I&C commits to obtaining and recording this from data subjects before processing commences.

Ultra I&C collects and processes information about data subjects as part of its day-to-day operations. This includes personal data relating to individuals who work for Ultra I&C in any capacity and personal data processed for customers, suppliers, partners and other parties.

All processing of personal data is undertaken in compliance with prevailing data protection and privacy law in the countries where we operate. This commitment is essential to ensure that personal data remains safe and the rights of data subjects are respected.

These laws include:

- UK – Data Protection Act 2018 and the General Data Protection Regulation (GDPR)
- Europe – the General Data Protection Regulation (GDPR)
- U.S. – US Federal Trade Commission and State legislation insofar as it is published, the California Consumer Privacy Act (2018) for example
- Canada – Personal Information Protection and Electronic Documents Act (PIPEDA) and equivalent Provincial law specifically the Quebec Privacy Act
- Australia – Australian Privacy Act (1988) and the Australia Privacy Principlesaddressed during the Bid approval process with adequate levels of internal scrutiny

Read our full Data Privacy Notice can be found on our website at www.ultra-ic.com.

Document Retention Policy

Ultra I&C businesses are required to maintain documents, records and other materials that are necessary to meet legal obligations, whilst promptly disposing of documents and records which are no longer necessary.

Where local rules dictate, a record of destruction of documents or records must be retained.

Each Ultra I&C business is required to maintain a database of all signed contracts.

Employee Records Retention Policy

Data protection law prohibits the retention of employee personal data for longer than is necessary. The period for retaining records is determined by the nature of the record and its contents. Ultra I&C is committed to data privacy and respecting the rights of data subject rights. Ultra I&C is committed to ensuring that personal data is only held for as long as it is needed before being securely disposed.

Ultra I&C data retention principles are:

- Legal retention – Ultra I&C complies with Data Protection and Privacy Legislation when storing records and will only store personal data for so long as it is necessary for a particular purpose.
- Limited retention – Ultra I&C limits historic retention of records and only stores documents needed.
- Maintained retention – Ultra I&C maintains records to ensure documents are regularly and systematically destroyed at the end of the retention period.
- Safe retention – Ultra I&C stores records in accordance with the Ultra I&C Information Security Policy. Records are stored appropriate to their classification and in a way that allows straightforward identification of the records.
- Justifiable retention – Ultra I&C only stores records beyond their retention period where justifiable.

Employee Code of Conduct

At Ultra I&C, we cultivate a culture of ethical conduct and workplace integrity that strengthens our relationships with employees, customers, and suppliers. This includes our willingness to maintain the highest standards in corporate governance, to go beyond the law in doing the right thing, to be always transparent and forthright in the conduct of our business.

Ethics and Business Conduct

Ultra Intelligence & Communications requires that all employees conduct themselves in ways that demonstrate high ethical standards in all of their dealings with customers, suppliers, governments, the public and each other. The integrity of Ultra I&C rests on the integrity of its employees.

Gifts and Corporate Hospitality Policy

Employees are permitted to offer modest non-cash gifts to business partners where appropriate for marketing purposes or, as long as the gift is occasional and not regular or repeated, other purposes such as expressing thanks or making a goodwill gesture.

Employees are permitted to accept token gifts from business partners or potential business partners where this constitutes legitimate and reasonable marketing or where it is a legitimate goodwill gesture.

However, if the giving or receiving of gifts or hospitality is in any way for the purposes of obtaining an inappropriate advantage or benefit, then this may amount to a bribe which is prohibited by the Gifts and Corporate Hospitality policy and by law.

The Gifts and Corporate Hospitality Policy sets out financial limits and approval levels for gifts and hospitality. It also outlines that both gifts and hospitality must be recorded in a gifts and hospitality register.

Information Security Policy

Ultra I&C ensures the confidentiality, integrity and availability of data is preserved through its adherence to certain principles which are applied to all information assets for which Ultra I&C businesses are responsible.

Each Ultra I&C employee is required to comply with the Acceptable Use Policy for computing services and facilities provided by or on behalf of Ultra I&C.

Offset Policy

Ultra Intelligence & Communications is committed to ensuring that any Offset activity in which it is involved is completed in full compliance with all applicable laws and regulations and in accordance with Ultra I&C's Anti-Corruption and Bribery Policy.

Ultra I&C businesses may only engage in Offset where they can demonstrate:

- there is no inherent risk of corrupt or unethical behaviour;
- appropriate due diligence has been conducted;
- there is a compelling justification for the level of Offset required; and
- internal approval has been obtained

Health and Safety Corporate Policy

Ultra I&C complies with all relevant statutory Health and Safety requirements in jurisdictions in which it operates.

Businesses are required to ensure that a suitable written Health and Safety Policy exists for their business and that the necessary organisational procedures and appropriate arrangements are in place to implement and support the policy.

All employees are responsible for taking reasonable care for his or her own Health and Safety and must ensure that they do not endanger the well-being of others by their acts or omissions.

Individual Rights Policy

Every individual whose personal data is held by Ultra I&C has rights in respect of that data. This includes individuals who work for Ultra I&C in any capacity as well as customers and business contacts. Ultra I&C supports the entitlement of individuals to exercise their rights to protect and verify the correct use of their personal data.

These rights are:

- Right of access (subject access requests) – the right to request a copy of the personal data that Ultra I&C has concerning the individual and supporting information explaining how the personal data is used.
- Right of rectification – the right to request that Ultra I&C rectifies inaccurate personal data concerning the individual.
- Right of erasure (right to be forgotten) – the right, in some situations, to request that Ultra I&C erases all personal data concerning the individual.
- Right to restrict processing – the right, in some situations, to request that Ultra does not use the individual's personal data they have provided (e.g. if they believe it to be inaccurate).
- Right to data portability – the right, in some situations, to request that Ultra I&C ports the individual's data to that individual or their new provider in machine readable format.
- Right to object – the right to object to certain processing of their personal data (unless Ultra I&C has overriding compelling grounds to continue the processing) and the right to object to direct marketing/profiling.

Ultra I&C's Data Protection Officer works with HR representatives and Privacy Champions to deliver rights requests ensuring compliance with prevailing data protection and privacy law. Rights requests are recorded via the Data Protection and Issues Log held within each business.

Legal Agreements Policy

Ultra I&C businesses are required to maintain:

- a register of all current legal agreements entered into by that businessa list of authorised signatories who can sign legal agreements on behalf of that business; and
- the level of authority delegated to each authorised signatory

Modern Slavery Policy

Modern slavery is the deprivation of a person's liberty by another in order to exploit them for personal or commercial gain. Ultra has a zero-tolerance approach to modern slavery and is committed to acting ethically and with integrity in all its business dealings and relationships.

Our full Modern Slavery Statement can be found on our website at www.ultra-ic.com.

OFAC and Sanctions Compliance Policy

All Ultra I&C businesses must comply with the economic or financial sanctions or trade embargoes administered or enforced by:

- the U.S. government, including those administered by the Office of Foreign Assets Control of U.S. Department of the Treasury (OFAC);

- the Canadian government, including the Minister of Foreign Affairs and the Canadian Department of Foreign Affairs, Trade and Development;
- the United Nations Security Council;
- the European Union; and
- Her Majesty's Treasury of the United Kingdom.

Personal Data Breach Response Policy

A personal data breach occurs where there is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. Ultra I&C has a duty to report personal data breaches to the relevant Supervisory Authority within the timeframe required by the Supervisory Authority. In the UK for example, Ultra I&C has 72 hours to report a data breach to the Information Commissioner's Office.

Aligned with Ultra I&C's commitment to safeguard all personal data, in the event a data breach is suspected, the Ultra I&C Data Protection Officer commences an investigation to determine whether a data breach has occurred, and whether it is likely to result in a high risk to a data subjects' rights and freedoms. Data subjects who have had their data compromised via a data breach are notified without undue delay with clear details including likely consequences and the measures to be taken.

Ultra I&C has appointed a network of Privacy Champions across the Company to establish, embed and encourage good practice within each Ultra business when dealing with the processing of personal data. Privacy Champions work in each business as first responders to support the implementation of data protection and privacy policies, support training and development activity and channel communications with the Ultra I&C Data Protection Officer. These individuals meet regularly and are trained and guided by the Ultra I&C Data Protection Officer to raise organisational awareness and help develop a positive data protection and privacy culture. Ultra I&C promotes and supports industry initiatives including the annual Data Privacy Day issuing newsletters and running other activities suggested and supported by Privacy Champions. All UK businesses have a Data Breach and Issues Log to record non-reportable data breaches and other personal data related issues occurring at an operational level. The Data Breach and Issues Log will be implemented across Ultra I&C globally by the end of 2021. Global Privacy Champions are also responsible for reporting data breaches to the Ultra I&C Data Protection Officer. Following investigation reportable data breaches are reported to the relevant Supervisory Authority by the Ultra I&C Data Protection Officer. Non-reportable breaches are recorded via the Data Breach and Issues Log.

The Ultra I&C Data Protection Officer collates data reported via the Data Breach and Issues Log and reports annually to the Executive Team. The reported measures include:

- Total time spent by Privacy Champions
- Data breaches non reportable (number of)

- Subject Access Requests (number of)Right to Erasure (number of)
- Policy / process / procedure rollout (time spent implementing)
- Training / development (time spent)

The Ultra I&C Data Protection Officer examines data submitted year on year to identify trends, emerging risks and areas for improvements.

Risk Management Framework

The Risk Management Framework provides a formal process to assist Ultra I&C in:

- Identifying the top level risks that can undermine the business model, future performance, solvency or liquidity of the Ultra I&C
- Developing and implementing procedures to ensure risks are identified and assessed against accepted criteria and that appropriate control and mitigation measures are implemented
- Defining and documenting responsibilities for Risk Management and reporting.

Ultra I&C has a very low appetite for risk where its culture, reputation or financial standing might be adversely affected.

Supplier Code of Conduct

Our Suppliers and their supply chains are critical to our ability to deliver customer commitments.

The Suppliers we engage with play an important role at every stage of the project lifecycle and are key stakeholders in Ultra I&C achieving successful business outcomes.

Ultra I&C commits to having a positive impact in our local communities, and we choose to work with Suppliers who have the same outlook.

Any business serious about environmental sustainability, ethics, compliance and monitoring its supply chain backs this up with a Supplier Code of Conduct. In engaging with Suppliers to Ultra I&C we need to be certain each party understands and accepts its responsibilities to fully comply with applicable laws and adhere to internationally recognised environmental, social, and corporate governance standards.

We encourage all our Suppliers to adopt the high standards Ultra lives by. We are working with our top 30 direct suppliers to obtain written representation that they commit to meeting the standards we have set out. Ultra I&C Procurement teams globally are working with all current and new Suppliers during the coming months seeking reliable representation they and their supply chain meet the standards set out in the supplier code of conduct:

- Anti-Bribery and Corruption
- Collective Bargaining
- Competitive behaviour and anti-trust
- Conflicts of interest
- Diversity, Equity, and Inclusion
- Export and Import controls, sanctions and obligations
- Fair pay and benefits
- Health, Safety and Environment

- Lobbying and political support
- Preventing facilitation of tax evasion
- Responsibly sourced materials
- Safeguarding confidential information
- Slavery, human trafficking and labour exploitation
- Working with stakeholders

While laws and regulations differ by location, we ask our Suppliers to always follow the spirit of the code in dealings with Ultra Intelligence & Communications and encourage open and transparent conversation with our Ultra I&C Procurement teams.

Please contact us with any questions about the Supplier Code of Conduct or Procurement.

Selection and Management of Intermediaries

Ultra Intelligence & Communications is subject to the stringent anti-corruption requirements of the US Foreign Corrupt Practices Acts (the "FCPA"), the UK Bribery Act (the "UKBA") and the local laws of the countries in which it operates. The FCPA and UKBA prohibit the bribery of foreign public officials by Ultra I&C or those working on its behalf.

Ultra Intelligence & Communications, in accordance with Regulator expectations, undertakes intermediary compliance reviews proportionate to the risks involved in the engagement of an intermediary.

Whistleblowing Policy

Employees are encouraged to raise any genuine concerns they might have about certain wrongdoings within the company without fear of reprisal.

The whistleblowing policy allows individuals to disclose any action or inaction by Ultra I&C or any of its workers, that the individual reasonably believes could lead or amount to:

- a criminal offence including bribery;
- a failure to comply with any legal obligations;
- a miscarriage of justice;
- danger to the health and safety of any individual;
- damage to the environment, or
- the deliberate concealment of information concerning any of the matters.

Disclosures may be reported using either of the following routes:

- directly to the individual's Line Manager
- via the employee Hotline – EthicsPoint