OPEN HEALTH

Global Ethical Business Conduct Code

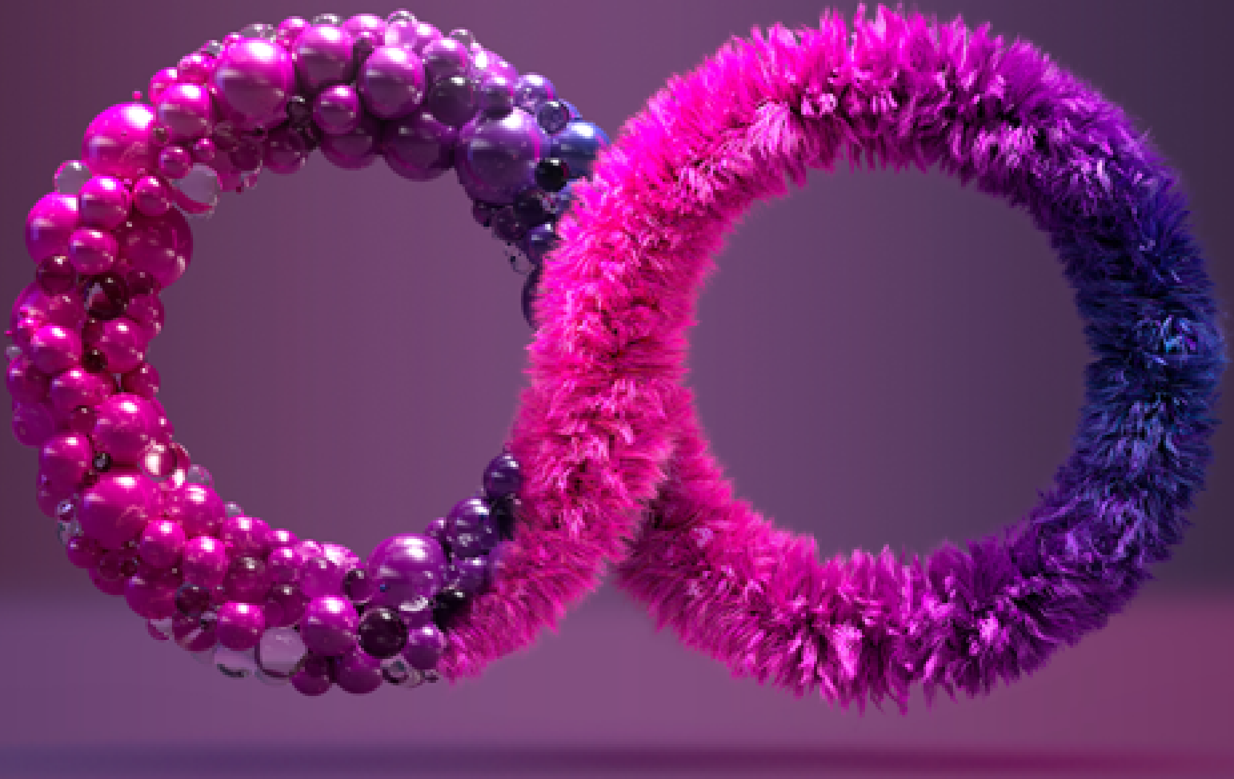


Table of Contents

03 Overview

04 Responsibility

05 Objectives

06 Expectations

07 Anti-Bribery and Anti-Corruption

08 Promoting Respect and Integrity

09 Human Rights and Anti-Slavery

10 Health and Safety

11 Alcohol and Substance Use

12 Environment, Social, and Governance (ESG)

13 Anti-Trust and Fair Dealing

14 Market Intelligence

15 Data Integrity and Study Participant Safety

16 Quality, Compliance, and Governance

17 Data Confidentiality

18 Insider Trading

19 Data Privacy

21 Use of Third Parties, Supplier Assessments, and Compliance Checks

22 Use of OPEN Health IT Assets

24 Public Communications and Social Media

25 Conflicts of Interests

26 Laws and Regulation, Including Healthcare

27 Policy of Non-Retaliation

Reporting, Whistleblowing and Ethics Helpline and Code of Conduct Breaches

28 Useful Contacts

Overview

This Code summarises OPEN Health's approach to Ethical Business Conduct and applies to all Staff including directors, officers, and temporary workers, whether full-time or part-time in any business location (and OPEN Health's Suppliers where indicated).

As a global enterprise with offices in many locations and countries, ensuring compliance with applicable laws and regulations in all the countries in which we do business is a core requirement. These include tax laws, accounting and financial reporting standards, and data protection laws, as well as healthcare sector, regional, and local requirements.

All Staff must be familiar with and comply with the laws, rules, and regulations applicable to their specific role whether local or global in nature.

No one is expected to know the details of all appropriate laws and regulations, but sufficient knowledge to determine when to seek appropriate advice from Line Managers, Human Resources, the Governance & Compliance Team, the Legal Team, or appointed internal or external experts is expected.

to top

Responsibility

The OPEN Health Executive Team is responsible for setting the strategic approach to this Code and accountable for ensuring its oversight.

Managers Are Responsible For Ensuring That Staff Are Aware Of:

- This Code
- Their own responsibilities for ethical business conduct
- The establishment of internal processes and procedures to uphold Code requirements
- The way to access advice on ethical business conduct
- Escalation requirements for non-compliance with this Code
- The potential for disciplinary action because of failure to comply with this Code

Managers Also Have Additional Responsibility To:

- Act as role models for ethical and responsible behaviour
- Respond promptly and effectively to any issues of non-compliance
- Review behaviour, practices, and approaches in areas of responsibility to ensure teams always act appropriately
- Ensure an open environment where Staff feel comfortable raising any concerns
- Commit to non–retaliation policies
- Report non-compliance

Staff at all levels are responsible for complying with this Code and related procedures and raising appropriate concerns as needed.

to top

Objectives

The Objectives Of This Global Ethical Business Conduct Code Policy Are To Ensure That:

- All Staff act with honesty and integrity
- All applicable legal, ethical, and regulatory standards are met
- Client services are delivered in an appropriate, compliant manner
- Regulatory requirements, including those applicable to the healthcare sector, are met
- Applicable internationally recognised standards, such as the Organisation for Economic Co-operation and Development Convention on Combating Bribery, are upheld
- Employment decisions are based on qualifications and merit
- Discrimination is prohibited in all jurisdictions (i.e., decisions based on any unlawful consideration such as age, race, national origin, gender, or other status protected by laws)
- Data integrity and privacy standards designed to protect patient safety are implemented

to top

Expectations

All Staff And Suppliers Are Required To:

- Always act with honesty, respect, integrity, and accountability
- Act in a professional manner that protects OPEN Health's reputation
- Understand and comply with OPEN Health policies
- Implement policies and processes specific to one's role, Centre of Excellence, or practice per geographical requirements
- Comply with laws, regulations, industry codes, policies, and procedures that relate to one's role
- Seek appropriate guidance when unsure of the correct manner in which to proceed according to the Code
- Be respectful and maintain a positive workplace free from harassment
- Complete assigned training and highlight personal or team training requirements proactively to line management
- Raise concerns promptly to the Governance & Compliance Team, Legal Team, or Ethics Line (see Section 23)

Staff Must Not:

- Engage in any unlawful or unethical activities
- Engage in illegal, fraudulent, defamatory, or malicious conduct

to top

Anti-Bribery and Anti-Corruption

OPEN Health does not tolerate bribery or any forms of corrupt practies.

OPEN Health prohibits all forms of fraud in its business operations and supply chain.

OPEN Health prohibits any form of money laundering and follows all anti-money laundering laws in all jurisdictions we operate in.

It is unlawful to make a payment to a government official to obtain or retain business or for a competitive business advantage.

Bribery of a non-governmental person (commercial bribery) is also prohibited in many countries.

Corrupt actions taken in one country may result in civil or criminal consequences not only in that country, but also in another. (e.g. USA and UK).

OPEN Health Staff and Suppliers must not give or receive bribes or engage in other corrupt practices, including attempting to change official decisions, win business, or gain an improper advantage.

All staff must comply with OPEN Health gifting and hospitality policies and related guidance and reporting procedures.

All Staff must complete Anti-Bribery and Corruption Prevention Training.

All suppliers must comply with OPEN Health's Supplier Code of Conduct, which forbids any acts of bribery or corruption and requires all supplier's staff members to be adequately trained in anti-bribery law and regulation in their trading territories.

to top

Promoting Respect and Integrity

Staff must treat each other with dignity and respect. OPEN Health believes in diversity of thought, culture, and background.

We will not tolerate any form of discrimination, harassment, or violence. Harassment includes unwelcome verbal, non-verbal, physical, or visual acts based on a person's status.

We respect the employment laws of each country in which we operate, and we recognise lawful employee rights, including applicable working hours, minimum wage standards, and the right to freely associate and collectively bargain where applicable.

We prohibit unlawful discrimination based on race, colour, creed, gender, religion, marital status, age, national origin or ancestry, genetic information, physical or mental disability, medical condition, sexual orientation, gender expression or identity, or any consideration made unlawful by federal, state or local laws with respect to recruitment, hiring, training, granting promotions, compensation, and other terms and conditions of employment.

to top

Human Rights and Anti-Slavery

OPEN Health is committed to protecting and advancing human rights globally.

We support the main principles of the International Labour Organization's Declaration on Fundamental Principles and Rights at Work, comprising of the elimination of forced and compulsory labor, child labor, human trafficking, discrimination, or any form of modern slavery on any part of our business or supply chain as well as creating a safe and healthy working environment.

OPEN Health's Anti-Slavery Statement and Supplier Code of Conduct are available on the website.

All staff and suppliers must report any concerns in this area to their manager, the Legal Team, The Governance and Compliance Team, or to the OPEN Health Whistleblowing and Ethics Helpline.

to top

Health and Safety

OPEN Health is committed to providing a work environment that protects employee physical health and safety as well as recognising and supporting mental health.

All OPEN Health Staff Must:

- Complete and comply with health and safety training, including in-office and work-from-home requirements as well as mental health and wellbeing training and signposting
- Follow any specific health and safety guidance or procedures issued applicable to one's role
- Read and follow any local Health and Safety Committee guidance provided and comply with all environmental, health, and safety laws

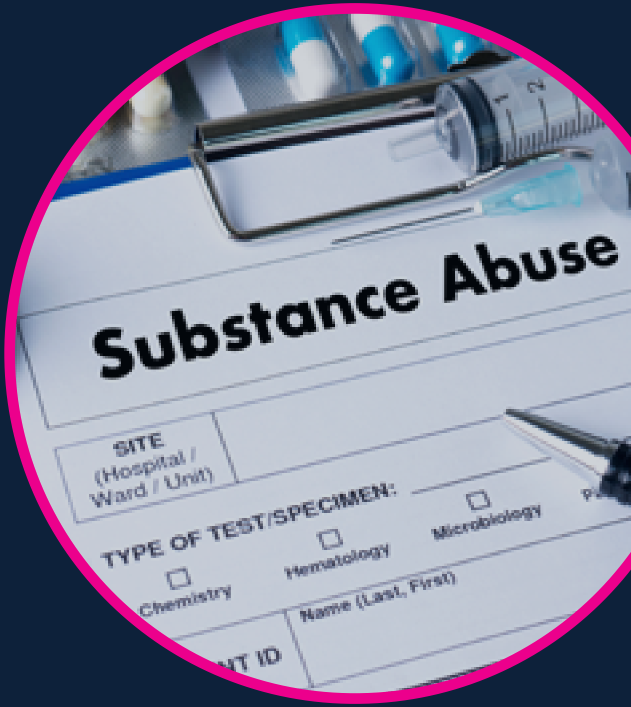
to top

Alcohol and Substance Use

OPEN Health prohibits working while impaired by the use of alcohol, illegal drugs, or other controlled substances. Substance and alcohol misuse pose serious health and safety risks not only to the users, but also to all Staff who work with them.

Staff may not possess any illegal drug or any legal prescription drug that is a controlled substance (unless the prescription has been issued to Staff and is being used in a manner consistent with the prescribed directions for use).

Staff may not possess or consume alcohol during working hours. Moderate alcoholic consumption within legal limits is allowed at organised team or social activity events organised by OPEN Health.



to top

Environment, Social, and Governance (ESG)

OPEN Health is committed to the core values of our ESG framework; to protect the environment, promote diversity and inclusion, and to operate our business with integrity and to report on our activities in our annual ESG report.

All OPEN Health Staff:

- Must follow all guidance provided on sustainability measures adopted by OPEN Health
- Are encouraged to identify opportunities to support ESG initiatives and identify carbon reduction opportunities to meet OPEN Health's published reduction targets
- Are requested to engage with our ESG team to promote ESG activities within our organisation
- Are encouraged to act in a manner that is sensitive to the environment, individual requirements and to speak up on non-conformance as needed

Anti-Trust and Fair Dealing

OPEN Health is committed to competing fairly based on the merits of our services and complying with relevant national and jurisdictional anti-trust laws. These laws require companies to compete independently rather than collaborate with competitors to unfairly restrain trade. Under these laws, certain practices must be avoided, including:

- Entering into formal or informal agreements or arrangements with competitors that would result in fixing prices to customers or Suppliers, adjusting sales volume, or dividing sales territories
- Exclusive arrangements with customers and Suppliers that inhibit competition or choice, such as agreeing that OPEN Health will not provide services regarding a specific dataset or patient group, or requiring that a vendor provide services only to OPEN Health, or prohibiting a supplier from increasing its prices to other customers
- Refusing to conduct business with a particular client or Supplier (or causing others to do the same) in order to obtain a better deal or rigging bids with competitors (including decisions not to bid)

Staff must not discuss, share, or agree prices, profit margins, costs, sales forecasts or plans, product supply, marketing, market share, territories, terms offered to particular clients or other sensitive marketing information (including marketing and business development strategies and plans with competitors), staff salaries, terms of employment, or benefits. However, such discussion, sharing, or agreement of any of the above is permitted if the action is taken in approved discussions covered by a trade association and with Legal Team approval.

Additionally, Staff must not make false statements, conduct contract interference, or suppress resource supply. Staff should only access confidential pricing or other commercially sensitive information if it is a requirement of their role for the performance of a business activity. The creation of personal copies of commercially sensitive information is prohibited.

to top

Market Intelligence

It is essential to our business to understand the business environment in which we operate, and this includes gathering market intelligence:

- Competitive intelligence can only be collected from sources other than the OPEN Health's competitors, such as publicly available information or non-Confidential Information from industry experts or other third parties. Where experts or third parties are used, avoid circumstances that could suggest the use of them as an intermediary to communicate with our competitors.
- If you become aware of Confidential Information about another company that has been disclosed, report and seek guidance from the Governance & Compliance and/or Legal Team.

to top

Data Integrity and Study Participant Safety

OPEN Health business units that provide research services are committed to ensuring that any research is scientifically valid, has an appropriate benefit-risk profile, includes informed consent as required, and is adequately overseen.

All OPEN Health Staff:

- Are required to maintain data integrity and comply with Data Integrity policies
- Must ensure that any data they manage are complete, consistent, and accurate throughout the data lifecycle, from creation through archival and destruction
- Are required to maintain all relevant healthcare and research standards, set out in section 23

All OPEN Health Suppliers of research services must comply with these standards and those set out in the Supplier Code of Conduct.

Quality, Compliance, and Governance

OPEN Health is committed to ensuring that we have standards of governance for quality and compliance for the provision of biopharmaceutical-regulated activities and pharmaceutical marketing and communications in all jurisdictions, including applicable laws and regulations.

Quality is a shared responsibility across OPEN Health and is integral to service delivery; all Staff are required to maintain applicable quality standards appropriate for their role.

Adherence to mandated compliance guidance and governance frameworks is a key responsibility of all Staff, including performing mandatory training on an annual basis.

Staff must also maintain adequate records to show adherence to required standards.

Data Confidentiality

Confidential Information is a valuable business asset that must be protected. OPEN Health's policies prohibit the use, duplication, modification, or disclosure of Confidential Information without appropriate written authorisation.

It is very important to safeguard OPEN Health's confidential and proprietary information as well as Confidential Information entrusted to us by other companies, and to use it only for appropriate purposes. Examples of Confidential Information include pricing plans, cost information, sales figures, financial results, employee data, customer lists, marketing and sales plans, other trade secrets, non-public financial information, business proposals, statistics, formulas, processes, inventions, and other intellectual property, whether that Confidential Information belongs to OPEN Health or any of its clients or Suppliers.

All Staff are required to sign a non-disclosure/confidentiality agreement agreeing to protect Confidential Information.

Staff Must Follow Good Practices To Protect Confidential Information, Including:

- Taking care when speaking or handling Confidential Information in public places such as trains, airports, restaurants, or through various public communication channels
- Taking care accessing and using mobile devices or systems and following IT security protocols and processes
- Only sharing Confidential Information outside OPEN Health if the third party has signed an appropriate confidentiality or non-disclosure agreement
- Ensuring accuracy of addresses on letters, packages, emails, and/or fax numbers prior to sending Confidential Information
- Reporting misdirected communications containing Confidential Information, Personal Data, or other inadvertent disclosure immediately to your manager and to dataprivacy@openhealthgroup.com

to top

Insider Trading

In addition to Confidentiality provisions all Staff are responsible to ensure they are aware of all relevant laws and regulations that prohibit “Insider Trading or Dealing,” which occurs when a person is in possession of material or non-public information and uses the information to sell or trade in shares or securities or provides information to others to enable trading. Staff must ensure that any trading activities carried out are clearly not attributable to receipt of information shared by Clients as part of their role in OPEN Health.

Data Privacy

OPEN Health processes Personal Data for a wide range of purposes. Personal Data relates to our Staff as well as third parties.

The protection of Personal Data is a key priority of OPEN Health in all jurisdictions, and it is essential that OPEN Health's Staff and Suppliers recognise their personal role in complying with data protection responsibilities and are familiar with the OPEN Health Global Privacy Policy. These responsibilities include:

a) Proper Purposes

- Staff must only collect the minimum amount of Personal Data required for the purpose and only use Personal Data processed in connection with our work for the purposes for which we obtained or created it
- Staff are responsible for deleting Personal Data promptly, in line with any client contractual requirements as well as the Global Data Retention Policy

b) Data Security

All Staff must maintain the security of Personal Data at all times and in all work locations, comply with OPEN Health's Information Security Policies, including Acceptable Use Policies and any associated procedures, and:

- At all times, use best efforts to physically secure any device against loss, theft, or use by persons not authorised to use the device
- Use strong passwords
- Use encryption of Personal Data in transfer
- Only store files or backup a device to an approved OPEN Health application or storage centre
- Must not use public unsecured Wi-Fi

to top

- Encrypt and/or password-protect documents containing sensitive Personal Data
- Only transfer Personal Data outside of the UK or EEA if you can confirm appropriate protections are in place to safeguard Personal Data (contact the Legal Team and/or the Governance & Compliance Team for guidance on contractual safeguards needed)
- Only disclose data to third parties that are authorised to receive it

Contractors who do not have access to the OPEN Health IT Assets and or infrastructure must comply with the Contractors IT Security Requirements available on the OPEN Health website.

c) Data Incident and Loss

As soon as an employee becomes aware that there has been a data incident or a suspected loss of OPEN Health data, including Personal Data, Confidential Information, or client data, it must be reported immediately by email to dataprivacy@openhealthgroup.com, and the relevant manager must be informed as set out in our Data and Security Incident processes and policies.

There are strict time reporting requirements in many territories for Personal Data breaches, so immediate reporting of a suspected incident is required by all Staff.

to top

Use of Third Parties, Supplier Assessments, and Compliance Checks

All Staff must follow policies in relation to vetting of third parties used as part of all business activities in the delivery of services. Third parties include clients, Suppliers, Contractors, agents, freelancers, and consultants.

All Staff must comply with Third Party Supplier Assessment policies.

Relevant due diligence is performed on third parties appropriate to their risk profile.

Where required, compliance checks are carried out on third parties, including checks for sanctions, PEPs (Politically Exposed Persons), and director identity checks. Further specific checks on individuals may be required under local legislation (e.g., FDA debarment checks in the USA).

For all third parties, appropriate contracts approved by the Legal Team must be used. If unsure, contact your manager or the Legal Team.

A Supplier Code of Conduct is in place to support third party integrity and accountability in their business practices.

to top

Use of OPEN Health IT Assets

OPEN Health IT Assets means all OPEN Health issued IT equipment or software for use in an office or remote location, including phones, computers, tablets, printers, systems, MACs, and related equipment to promote effective working and for business continuity purposes. Appropriate use for productive business purposes is a key requirement. Any user of OPEN Health's IT Assets must take reasonable steps to protect IT Assets against theft. IT Assets must be treated with care and used only for appropriate legitimate business purposes in an ethical manner in line with applicable IT policies and these standards. IT Assets cannot be used to:

IT Assets Cannot Be Used To:

- Violate any OPEN Health policy, Code, or procedure
- Perform any activity that may bring the reputation of OPEN Health into disrepute or to defame or discredit OPEN Health, its clients, business partners, or Suppliers
- View, send, receive, or store illegal, offensive, obscene, or defamatory materials or publish non-authorised OPEN Health materials
- Monitor or intercept files or electronic communications of other Staff without prior authorisation
- Download or use unauthorised applications

to top

a) Temporary Staff

Any temporary staff or Contractors, not using OPEN Health's IT (if authorised in writing) must adhere to this Code, the OPEN Health Acceptable Use Policy, and the Contractor Information Security Policy available on the OPEN Health website.

- Ensure up-to-date anti-virus or anti-malware software is installed on any equipment used
- Protect the device with a PIN or strong password, keep the PIN and password secure, and change the PIN and password frequently
- Refrain from downloading or transferring any Confidential Information (including Personal Data) onto a portable removable device or e-mail attachment, unless specifically authorised to do so
- Ensure that Confidential Information is encrypted using appropriate encryption technologies wherever stored
- Use a secure method to transfer or share data approved by the OPEN Health IT Team

b) Lost or Stolen Devices and Unauthorised Access

In the event of a lost or stolen IT Asset or any portable removable device in use or where Personal Data or Confidential Information is believed to have been accessed unlawfully or compromised, the Staff member must report the incident to the IT Department AND dataprivacy@openhealthgroup.com immediately.

to top

Public Communications and Social Media

All communications made on OPEN Health's behalf on social media channels (including internal chat functions) needs to be appropriate and approved in line with this Code, the Global Social Media Policy, the Global Privacy Policy, and relevant guidance issued by healthcare regulators.

Staff Are Prohibited From Using Any Social Media, Personal, or Business Channel To:

- Harass or bully other Staff in any way
- Breach privacy laws (e.g. disclosing Personal Data about a colleague online)
- Breach regulatory rules and requirements (e.g. the Association of British Pharmaceuticals and the Pharmaceuticals Research and Manufacturers Association [PhRMA])
- Breach confidentiality obligations
- Make a false or misleading statement about, defame, or disparage OPEN Health or its customers, clients, employee's business partners, Suppliers, vendors, or other key stakeholders

For queries on approvals for business-led social media content, please contact: marketing@openhealthgroup.com.

to top

Conflicts of Interest

a) Personal

OPEN Health respects the rights of our Staff and our Suppliers to be involved in activities outside the scope of their role at OPEN Health, provided these activities do not conflict with their work responsibilities. Conflicts can arise in a variety of ways, for example:

- Financial conflicts of interest (e.g. a financial interest in any customer, potential customer, supplier/vendor, or OPEN Health competitor)
- Employment: being an employee, officer, or director of any supplier, customer, or OPEN Health competitor without prior written approval from OPEN Health
- Family member: supervising or influencing the performance evaluation or compensation of a family member who is an employee of OPEN Health

b) In Business

OPEN Health is committed to managing potential competing client conflicts in a professional and ethical manner when working in research or providing services in relation to research and other agency and communications services.

All Staff must comply with established processes to manage any actual or potential conflict.

Managers should be contacted for guidance and possible conflict situations should be raised with the Legal Team and/or Governance & Compliance Team at the earliest opportunity.

Staff are prohibited from using confidential or proprietary information or intellectual property of OPEN Health or our customers for personal gain.

OPEN Health Staff and Suppliers must disclose any actual or potential conflicts of interest as soon as they arise, whether “personal” or “in business,” to their line manager (Staff) or designated OPEN Health contact (Suppliers).

to top

Laws and Regulation, Including Healthcare

OPEN Health's business is subject to laws and regulation in all territories, including some specific healthcare requirements in the delivery of its services.

All Staff must seek advice from the Legal Team and/or the Governance & Compliance Team if unsure as to what laws may apply.

to top

Policy of Non-Retaliation

OPEN Health operates a strict non-retaliation policy, protecting people who raise concerns or seek advice. This enables issues to be raised and reported in good faith. For example, Staff can participate in an investigation, and no negative actions will be taken against them.

Reporting in “good faith” means the reporter reasonably believes that the information relayed shows misconduct, non-compliance with a business practice that could cause serious harm or give rise to liability, or a violation or suspected violation of this Code or any applicable law or regulation including but not limited to pharmaceutical regulation, laws prohibiting employment discrimination, accounting standards, accounting controls, and audit procedures, within OPEN Health, or by any client or supplier.

Reporting, Whistleblowing and Ethics Helpline and Code of Conduct Breaches

All Staff have access to an external reporting helpline, (Whistleblowing and Ethics Helpline) allowing Staff an independent confidential option to report which can also be anonymous.

If any Staff member becomes aware of a breach of this Code, the incident must be reported immediately to the Governance and Compliance Team and/or the Human Resources Team or via the Ethics Helpline.

Breaches of this Code by Staff may result in disciplinary procedures.

to top

Useful Contacts

Governance and Compliance Team:
GovernanceandCompliance@OpenHealthGroup.com

Legal Team:
LegalandContracts@OpenHealthGroup.com

For Data Breaches - Data Privacy Email:
DataPrivacy@OpenHealthGroup.com

IT Department:
ITGovernance@openhealthgroup.com

Marketing:
Marketing@openhealthgroup.com

Whistleblowing and Ethics Helpline:
Details available on the Governance & Compliance ORBIT site

to top

OPEN HEALTH

to top