Oneview / the connected care experience company

Oneview Healthcare PLC (ASX: ONE) ABRN: 610 611 768

CODE OF CONDUCT
2026

Oneview Healthcare PLC and its subsidiaries (the Company)

Version	**2.0**
Date of Version	**29 Jun 2026**
Created By	**Company Secretary**
Approved By	**Management**
Confidentiality Level	**TLP:GREEN**

Oneview Healthcare PLC is an Irish company registered under the Companies Act 2014 as a public limited company (513842). It is registered under the Corporations Act 2001 (Cth), Australian Registered Body Number 610 611 768.

1. Introduction

1.1 Background

The Company is committed to maintaining ethical standards in the conduct of its business activities. The Company's reputation as an ethical business organisation is important to its ongoing success. The Company expects you to be familiar with and have a personal commitment to meeting these standards. These standards go beyond mere compliance with laws and regulations. They also embrace the values which are essential to the Company's continued success.

1.2 Purpose

This Code of Conduct (**Code**) clearly states the standards of responsibility and ethical conduct expected of you as a director or employee of the Company. It applies to all directors and employees of the Company, and where relevant and to the extent possible, consultants, secondees and contractors of the Company.

The Code requires you and, where relevant and to the extent possible, consultants, secondees and contractors of the Company to adhere to the law and various policies of the Company referred to in this Code. The standards set out in this Code cannot, and do not try to, anticipate every situation which may pose a legal, ethical or moral issue. Therefore, the Code is not a prescriptive set of rules for business behaviour, but rather a practical set of principles giving direction and reflecting the Company's approach to business conduct.

You need to exercise sound judgment when evaluating an issue of business conduct. If you are in any doubt, you should seek advice before taking any action which may compromise yourself or the Company.

For personnel and contractors involved in the Oneview Care Experience Platform or related control activities, this Code also supports Oneview's ISO 27001, ISO 27701 and SOC 2 control environment. Those individuals must follow applicable information security, privacy, confidentiality, availability, change management, incident reporting, access control, supplier management and evidence-retention requirements that support the scoped production service and related Trust Services Criteria.

2. The Company's business ethics

2.1 Openness, honesty, fairness, integrity and in the best interests of the Company

You must conduct yourself with openness, honesty, fairness, integrity and in the best interests of the Company in all business transactions and in all dealings with others including customers, suppliers, shareholders, employees, joint venture partners, creditors, financiers, the financial markets, investors, governments and the general public.

This means that you:

(a) must not make promises or commitments which to your knowledge the Company is unable to, or does not intend to, honour;
(b) must ensure that all business decisions with customers and suppliers are made solely on sound commercial grounds having regard to the quality, price and service;
(c) must not use the Company's name or your position for personal gain or in

competition with the Company;

(d) must act with due care and diligence in fulfilling the functions of your office or employment; and

(e) should not engage in conduct which may bring discredit upon the Company.

2.2 Giving and accepting business courtesies

You must not give, seek or accept in connection with the Company's operations any gifts, meals, refreshments and entertainment which goes beyond common courtesies associated with ordinary and proper course of business. You must avoid everything that could reasonably be construed as a bribe or improper inducement.

Any gift, entertainment or other personal favour or assistance given or received which has a value in excess of €500 (or its equivalent in any other currency) (or any other amount determined and announced by the Board) must be approved by the CEO or CFO and entered into the gifts register maintained by the CFO. Any gift not declared may be viewed as a bribe.

The rationale for this restriction is that the offer or acceptance of a gift can create an obligation or be construed or used by others to allege favouritism, discrimination, collusion or similarly unacceptable practices by the Company.

2.3 Financial and other inducements

Offering a bribe to a government official and the receipt of a bribe by a government official is prohibited under Irish law and the laws of most countries. Ireland is a signatory to the OECD Convention Combating Bribery of Foreign Public Officials in International Business Transactions and has enacted legislation prohibiting the offering of anything of value to foreign public officials which enables it to prosecute its citizens and corporations for the bribery of public officials in other countries.

A contravention of anti-bribery legislation has serious consequences, such as imprisonment or fines.

You should not make any payments or payments in kind (gifts, favours, etc.) to influence individuals to award business opportunities to the Company or make business decisions in the Company's favour.

2.4 Mutual respect

You are expected to treat with courtesy and respect your colleagues, joint venture partners, customers, shareholders and anyone else with whom you interact in your work.

2.5 Ethical conduct

You must act ethically in your approach to business decisions.

In negotiating and administering contracts and other business relationships, you are expected to be fair and reasonable. You must not behave in any way that is, or might be construed as being harsh, oppressive, unconscionable, unethical, coercive or dishonest.

3. Business and personal conduct

3.1 Compliance with laws and regulations

You must comply with all laws and regulations relating to your business conduct and the Company's operations. This includes being familiar with the duties and responsibilities applying to you under the laws relevant to the Company and in the context of your role in the Company.

Any activities carried out by yourself or the Company outside Ireland must comply with the foreign laws which may apply to any activities or operations.

Each member of the leadership team is required to ensure that they are aware of the legal obligations and requirements that impact their areas of responsibility.

The laws that govern the Company's business activities may be complex. You are encouraged to contact the Company Secretary or the Company's General Counsel if you are unclear about laws or regulations relating to your work. There can be no justification for knowingly breaking the law or for choosing to be uninformed about the law. Good motives are not an excuse for committing illegal acts.

3.2 Trading in Shares

The law prohibits dealing in the shares of a company while in possession of "inside information". "Inside information" is information that is not generally available and if it was available, a reasonable person would expect it to have a material effect on the price or value of Company shares.

You must not (and must not cause another person to) trade in the Company shares or the shares of any other company to which the information relates on the basis of inside information or pass inside information onto some who might use inside information to trade in the Company shares or any other company to which the information relates.

A breach of insider trading provisions may result in criminal prosecution.

Any trading or other dealing in the Company shares must be done in accordance with the Securities Trading Policy. If you have any doubt, you should contact the CFO or Company Secretary.

3.3 Privacy and Intellectual property

You may have access to records which contain information that may be of a personal nature, or that the Company has obtained to assist in the management of the business. This information is private and confidential and may not be disclosed to any unauthorised third party.

All intellectual property that you generate in relation to the Company and its activities is the property of the Company. You are responsible for protecting the Company's intellectual property rights.

3.4 Confidentiality and control of information

3.4.1 Protection and authorised use

You must ensure that you do not disclose any Confidential Information or Proprietary Information to any third party or other employee who does not have a valid business reason for receiving that information.

"Confidential Information" in this context means information that the Company considers private and that is not generally available outside the Company.

"Proprietary Information" in this context means information that the Company owns, develops, pays to have developed or to which it has an exclusive right.

If Confidential Information or Proprietary Information is required to be provided to third parties or other employees for valid business purposes, the Company and its employees must:

(a) take adequate precautions to ensure that information is only used for those purposes for which it is provided and is not misused or disseminated to the Company's detriment; and
(b) ensure that the information is returned or destroyed when the purpose is complete.

Such precautions include obtaining a confidentiality agreement or other undertaking. Advice about these measures can be obtained from the CFO or Company Secretary.

3.4.2 Scoped service information and control evidence

Confidential Information includes customer information, personal data, protected health information, restricted configuration data, application-generated operational data, system and audit logs, monitoring data, support records, security evidence, access records, change records, incident records and other information used to operate or evidence controls for the Oneview Care Experience Platform. Information relating to the scoped production service must be handled in accordance with the Data Classification Policy, customer and regulatory obligations, and applicable security and privacy procedures.

Access to scoped service information and control evidence must be limited to authorised personnel with a valid business need and must not be shared outside approved systems, approved recipients or agreed customer, auditor, legal, regulatory or subservice organisation processes. Personnel must not bypass approved access control, change control, deployment, monitoring, logging, support or evidence collection processes for convenience or speed.

3.4.3 Return, disposal and retention

You must:

(a) return all Company property including any documents or Confidential Information or Proprietary Information, on termination or on the request of the Company or its representative; and
(b) if requested by the Company or its representative, destroy or delete any Confidential Information or Proprietary Information stored in electronic, magnetic or optical form so that it cannot be retrieved or reconstructed.
(c) retain, return, delete or dispose of Company, customer and scoped service information only in accordance with approved retention schedules, legal hold requirements, contractual obligations and documented disposal procedures.

3.5 Corporate opportunities

You must not, without written approval of a member of the leadership team, pursue or take personal advantage of any business opportunities which arise as a result of your position

within the Company or the use of the Company's property or information.

3.6 Financial integrity

The Company has stringent financial accounting procedures that are overseen by management, the Audit Committee and the external auditor. Therefore:

(a) the use of Company funds or assets for any unauthorised or unethical purpose, including for the advantage of others, or to cause loss to the Company is prohibited. No undisclosed funds or assets of the Company have, or will be, maintained or established for any purpose;

(b) no false or misleading entries may be made in the books or records of the Company for any reason; and

(c) no payment on behalf of the Company may be made or approved on the understanding that it will or might be used for something other than the stated purpose.

You must ensure that:

(a) the Company's financial books, records, reports and statements properly document all assets, liabilities, and revenue; and

(b) expenses accurately reflect all transactions of the Company and are retained in accordance with the Company's policies and all applicable laws and regulations.

3.7 Personal conduct

You are expected to adhere to the following standards of personal conduct:

(a) act honestly, in good faith and in the best interests of the Company as a whole;

(b) use due care and diligence in fulfilling the functions of your position and exercising the powers attached to your employment;

(c) recognise that your primary responsibility is to the Company and its shareholders as a whole;

(d) attend and undertake your work without being under the influence of drugs, alcohol or other substances or being distracted by personal business or other interests; and

(e) protect any Company assets under your control and not use them for personal purposes, without the Company's prior approval.

3.8 Business agreements and contracts

The Company expects to compete fairly and ethically for all business opportunities. If you are involved in the negotiation of agreements on behalf of the Company or an entity controlled by the Company:

(a) you must ensure that you act in accordance with the law;

(b) all statements, communications and representations made to customers, suppliers, partners, competitors and others with whom you undertake business transactions, should be accurate and truthful and must not be misleading or deceptive;

(c) all appropriate approvals must be obtained before any agreements are executed; and

(d) you acknowledge that the Company is committed to meeting all of its contractual obligations and accordingly you are expected to know, understand, and honour the terms of the Company's contractual obligations that are relevant to your role.

(e) you must not make commitments about security, availability, confidentiality, privacy, system scope, service levels, processing activities, subservice organisations or customer responsibilities unless those commitments are approved, accurate, consistent with contractual terms and aligned with the current scoped service description and supporting policies.

3.9 Gathering information on the company's competitors

While the Company acknowledges that an understanding of the market, and therefore its competitors, is essential in undertaking business, gathering this information should be done legally and ethically. Information should not be gained through unlawful or deceitful means.

3.10 Avoiding or managing conflicts of interest

A conflict of interest arises when a person is in a position which requires them to balance their own interests or the interests of others (such as friends or relatives)against the interests of the Company. You must fully and promptly disclose to the Company any private or other business interests or other matters which may lead to potential or actual conflicts of interest.

If you have any doubt about conflicts of interest, you should contact the CFO or Company Secretary, in the case of directors and a member of the leadership team, or your manager in the case of any other employee.

3.11 The financial community

The Company is committed to delivering shareholder value within an appropriate framework which safeguards the rights and interests of the Company's shareholders and the financial community generally. The Company aims to comply with the systems of control and accountability in place as part of its corporate governance in accordance with the ethical standards referred to in this Code.

3.12 The Company and its employees

The Company actively supports the principle of equal employment opportunity regardless of race, religion, national origin, sex, age, physical disability, marital status or sexual orientation and expects its senior management and employees to practice and support this principle.

The Company's policy is to avoid discriminatory practices of any kind and to make employment and career decisions strictly on the basis of individual ability, performance, experience and Company requirements.

The Company believes that every individual has the right to dignity and respect in the workplace. Therefore, the Company regards any personal, physical or sexual harassment as totally unacceptable. That sort of behaviour is unacceptable regardless of whom the perpetrator is, and may lead to the termination of their employment. The

use of any medium (including email or the Internet) to disseminate material which is sexually explicit, defamatory, vulgar, or racist is prohibited. The use of Company facilities to access material which is sexually explicit, defamatory, vulgar, or racist is also prohibited. These policies apply to you regardless of your position.

3.13 Respectful use of systems and information

Company systems, customer systems, scoped service environments, client device management platforms, monitoring tools, development tools, deployment tools and evidence repositories must be used only for authorised business purposes. Personnel must protect credentials, use approved authentication methods, comply with role-based access restrictions, report suspected misuse or compromise promptly, and must not intentionally disable, evade or weaken security, monitoring, logging, endpoint management or privacy safeguards.

The Company is committed to protecting the health and safety of its employees, visitors and the public. The Company expects and requires you to comply with Occupational Health and Safety laws and Company policies, including your obligation to report any hazardous conditions in the workplace and any workplace incidents or accidents.

3.14 Other policies regulating employee behaviour

3.14.1 Security, privacy and operational policies

The Company has policies and procedures which govern conduct of its business and operations. All senior management and employees are expected to make themselves familiar with the Company's policies and procedures and to adhere to those policies in conducting business or operations on behalf of the Company.

You are also expected to know, and always act within, the limits of your authority to speak on behalf of the Company and to commit the Company to business transactions or to make other commitments on behalf of the Company.

Where your role supports the Oneview Care Experience Platform or related corporate controls, you must comply with applicable information security, privacy, data classification, access management, change management, software development, incident response, business continuity, supplier management, acceptable use, records retention and evidence management policies and procedures. Failure to follow those requirements may affect Oneview's ability to meet ISO and SOC 2 commitments and may be treated as a breach of this Code.

4. Other matters

4.1 Compliance

4.1.1 Reporting concerns

It may be difficult to always ensure compliance with this Code and therefore the cooperation of every person is required. If you suspect that any fraudulent or unethical behaviour has occurred, or are concerned that any conduct by any director, officer or employee may be in breach of applicable law or this code, you should contact the Chair of the Audit Committee, the CFO, Company Secretary, or the Company's auditors. Details of any concerns and the identity of any persons making the report will be treated confidentially. Any matter reported will be handled promptly and in a manner that ensures the individual is not disadvantaged for reporting their concerns. For full details, please see the Company's Whistleblower Policy. Employees may receive

training on how to comply with the Code.

Suspected or actual security incidents, privacy incidents, unauthorised access, data loss, inappropriate disclosure, control failures, circumvention of approved procedures, inaccurate evidence, or material issues affecting the availability, confidentiality, privacy or security of the scoped service must be reported promptly through the applicable incident, management, legal, compliance or whistleblower reporting channels.

4.2 Consequences for breaching the code

4.2.1 Investigation and remedial action

All suspected breaches of the Code will be thoroughly investigated by the Company. If these investigations reveal breaches of the Code, appropriate disciplinary and remedial action will be taken, depending on the nature of the breach. This will range from providing the director, senior manager or employee with training, coaching and counselling through to formal warnings and/or to termination.

Where a breach relates to information security, privacy, service availability, confidentiality, system access, customer information, control evidence or scoped service operations, remedial action may include access removal, control correction, evidence remediation, customer or regulator notification where required, supplier follow-up, retraining, disciplinary action, and updates to policies, procedures or risk treatment plans.

The Company reserves the right to inform the appropriate authorities where it is considered that there has been criminal activity or an apparent breach of the law.

4.3 More information

If there are any questions regarding any aspect of this Code, please contact the Company Secretary or CFO.

4.4 Amendment of policy

This Policy may be amended by management from time to time to reflect operational, regulatory or best practice developments. All material amendments will be subject to Board approval. A summary of amendments will be provided to the Board for review on at least an annual basis.

Material amendments affecting information security, privacy, confidentiality, availability, customer commitments, regulatory obligations or the scoped SOC 2 control environment must be reviewed by the relevant governance, legal, compliance, security or privacy stakeholders before approval.

4.5 Adoption of Policy and Board review

This Code of Conduct was adopted by the Board on 17th February 2016 and takes effect from that date and replaces any previous policy in this regard.

The Board will review this Code of Conduct periodically. The CEO, CFO or Company Secretary will communicate any amendments to employees as appropriate. This Code was last reviewed on 29th June 2026 and replaces any previous policy in this regard.