

# GROUP POLICY

# Code of Conduct



# Diploma PLC

## Code of Conduct

### Message from the CEO

#### OUR VALUES

Our Group values are a set of guiding principles that reflect the shared beliefs and behaviours of our businesses and set the tone for our culture.

##### **Customer-centric**

We are driven to add value and help our customers grow.

##### **Grow together**

We collaborate to create success and opportunity.

##### **Do the right thing**

We are ambitious about delivering value responsibly.

##### **Down to earth**

We are low on ego – our performance speaks for itself.

##### **Accountable**

We are all empowered to succeed.

At Diploma, how we work matters just as much as what we achieve.

This Code of Conduct reflects our shared commitment to act with integrity, take responsibility, and always do the right thing - for our colleagues, customers, suppliers, and communities. It's a practical guide to help you make decisions that align with our values, comply with the law, and support long-term success.

Our decentralised model means decisions are made close to the customer - but we all uphold the same standards. Whether you're working in operations, sales, procurement, or support, we each have a role in protecting Diploma's reputation and building a business we're proud of.

Please take the time to read the Code, complete the training, and speak up if something doesn't feel right. Your actions matter, and together we can ensure Diploma continues to be a trusted, responsible and high-performing organisation.

Thank you for your continued commitment.

Johnny Thomson  
Group CEO  
June 2025

# Contents

|                                                               |    |
|---------------------------------------------------------------|----|
| Our Code of Conduct.....                                      | 2  |
| Raising Concerns and Whistleblowing.....                      | 3  |
| Delivering Value Responsibly.....                             | 4  |
| Delivering for Our People .....                               | 5  |
| 1 Diversity, Equity and Inclusion .....                       | 5  |
| 2 Colleague Engagement .....                                  | 5  |
| Doing Business Responsibly.....                               | 6  |
| 3 Personal Integrity.....                                     | 6  |
| 3.1 Conflicts of Interest.....                                | 6  |
| 3.2 Insider Trading and Share Dealing .....                   | 7  |
| 3.3 Gifts, Hospitality and Entertainment .....                | 7  |
| 3.4 Anti-Facilitation of Tax Evasion.....                     | 8  |
| 4 Commercial Integrity.....                                   | 8  |
| 4.1 Fair Competition and Anti-Trust.....                      | 9  |
| 4.2 Anti-Money Laundering .....                               | 9  |
| 4.3 Sanctions and Export Controls .....                       | 10 |
| 4.4 Bribery and Corruption .....                              | 10 |
| 4.5 Fraud – Including Failure to Prevent Fraud.....           | 11 |
| 4.6 Charitable and Political Donations .....                  | 13 |
| 4.7 Responsible Tax Conduct.....                              | 13 |
| 4.8 Accurate Records and Financial Responsibility.....        | 13 |
| 5 Safeguarding Information and Systems.....                   | 14 |
| 5.1 Information Security .....                                | 14 |
| 5.2 Use of Technology and Cybersecurity .....                 | 14 |
| 5.3 Use of Artificial Intelligence and Automation Tools ..... | 15 |
| 5.4 Intellectual Property.....                                | 15 |
| 5.5 Data Privacy and Protection .....                         | 15 |
| 5.6 Responsible Communication and Social Media .....          | 15 |
| 6 Health & Safety.....                                        | 16 |
| 6.1 Product and Service Safety .....                          | 16 |
| 6.2 Business Continuity and Crisis Preparedness.....          | 17 |
| 7 Human Rights and Modern Slavery .....                       | 17 |
| 8 Working with Partners .....                                 | 18 |
| 9 Third Parties and Associated Entities.....                  | 19 |
| Delivering for the Environment .....                          | 20 |
| Our Policy Library .....                                      | 21 |
| Contacts and Support .....                                    | 22 |
| Code of Conduct Declaration.....                              | 23 |

## Our Code of Conduct

### Purpose and Scope

This Code sets out the standards of behaviour expected from everyone working for or on behalf of Diploma. It helps us act with integrity, comply with the law, and maintain the trust of our colleagues, customers, suppliers, investors, and communities.

The Code applies to all Group colleagues, directors, contractors, and anyone representing Diploma across our businesses. You are expected to read and understand the Code, apply it in your day-to-day decisions, and ask for guidance if anything is unclear.

The Code is reviewed annually to ensure it reflects current laws, emerging risks, and best practices. Updates are approved by the Board and communicated across the Group.

### Living Our Values

Our Code is built on Diploma's values. These guide how we behave, make decisions, and work with others every day. They underpin our commitments to our people, responsible business, and sustainable growth.

This Code is not an exhaustive list of rules, but a practical framework to help you make the right choices. It works alongside our Group policies and the laws of the countries in which we operate.

If you're ever unsure what's expected, pause and ask. Speak to your manager, local leadership, or contact the Group (see Contacts).

Living our values protects you, your colleagues, and the Group - and strengthens the trust others place in us.

### Communicating and Upholding the Code

All colleagues are introduced to this Code during onboarding and is accessible through the Diploma website and the Learning Management System "Purple Portal".

Each Diploma business is responsible for ensuring:

- All colleagues are aware of the Code and receive role-appropriate training
- The Code's principles are consistently applied across operations
- Third parties acting on our behalf understand and uphold the Code

Colleagues must complete Code of Conduct training when joining, with additional and refresher modules assigned based on role and risk level. For help with access to the Purple Portal, contact Group HR.

Living the Code is everyone's responsibility. Managers must lead by example and support its application in their teams.

Breaches of the Code, related policies, or laws may lead to disciplinary action, including dismissal, legal action, or ending relationships with third parties.

## Raising Concerns and Whistleblowing

We are committed to a culture of openness and integrity. If you see or suspect wrongdoing – such as unethical conduct, legal breaches, or policy violations – you have the right to raise a concern.

Anyone can report a concern: colleagues, suppliers, contractors, former employees, or the public.

You can raise concerns with:

- Your line manager
- Your Managing Director
- Group Legal or Group HR

Or report confidentially or anonymously through the Diploma Confidential Hotline, operated 24/7 by independent provider Safecall:

- Online: [www.safecall.co.uk/file-a-report](http://www.safecall.co.uk/file-a-report)
- Email: [diploma@safecall.co.uk](mailto:diploma@safecall.co.uk)
- Phone: Call your country's freephone number (listed on the Safecall website)

Your rights are protected:

- Reports are confidential
- You may remain anonymous
- You don't need proof – just a genuine concern raised in good faith
- Retaliation is not tolerated against anyone who speaks up or supports an investigation

Safecall posters must be clearly displayed in all workplaces so everyone knows how to raise concerns.

For more information, refer to the Group Whistleblowing Policy or contact Group General Counsel (see Contacts).



## Delivering Value Responsibly

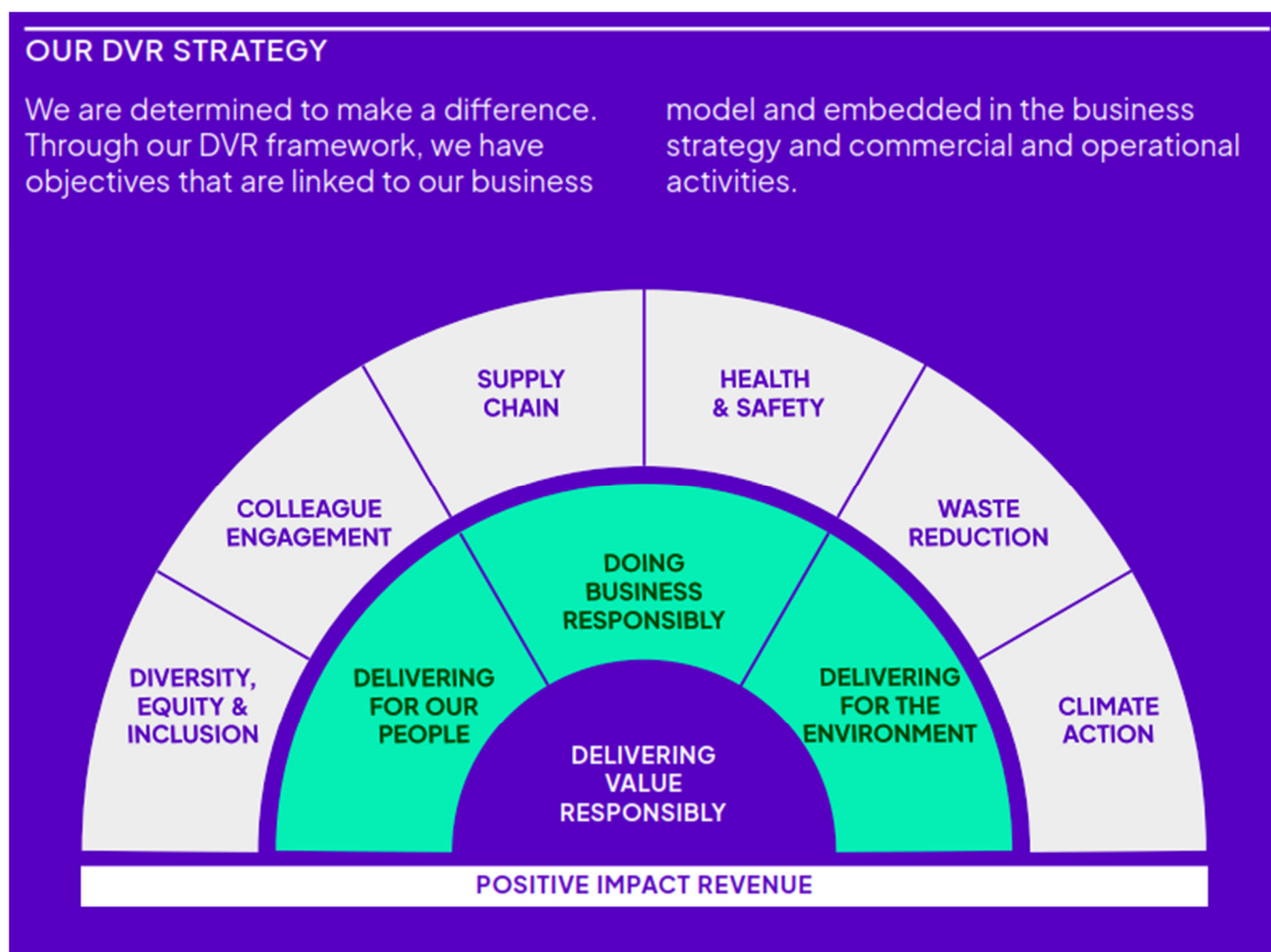
Our Delivering Value Responsibly (DVR) framework is integrated across our businesses, focusing on three key areas:

- Delivering for Our People
- Doing Business Responsibly
- Delivering for the Environment

By concentrating the efforts of our large, diverse, and decentralised Group on these core areas, we can drive meaningful progress against our sustainability targets.

To support this framework, the Group's policies are also structured around these three pillars.

This ensures alignment between our day-to-day behaviours, strategic goals, and compliance requirements – so that the way we operate is consistent, transparent, and values-led.



## Delivering for Our People

### 1 Diversity, Equity and Inclusion

Diploma is committed to creating a workplace where everyone is treated fairly and respectfully. We support diversity in all its forms and strive to ensure that every colleague feels included, valued, and able to succeed.

Discrimination, harassment, or bullying of any kind will not be tolerated. This includes discrimination based on age, race, ethnicity, gender, sexual orientation, gender identity, disability, religion, marital status, pregnancy, or any other protected characteristic.

Each business must:

- Maintain a local DEI policy or plan tailored to its size and legal obligations
- Promote inclusive behaviours in day-to-day decisions and operations
- Ensure fair and unbiased recruitment and promotion practices
- Provide DEI training for managers, HR teams, and recruiters
- Communicate DEI commitments clearly and encourage feedback and dialogue
- Offer trusted and accessible channels to report concerns

Our goal is to improve representation – especially in leadership – and to embed DEI in how we operate and grow. If you experience or witness exclusion or unfair treatment, speak to your manager or use the Whistleblowing service.

For more information, refer to the Group DEI Policy or contact Group HR (see Contacts).

### 2 Colleague Engagement

We want every colleague at Diploma to feel informed, empowered, and proud of the work they do. Open, respectful, and inclusive communication helps keep us connected – across teams, businesses, and geographies.

Leaders are expected to promote regular, transparent engagement through local updates, team meetings, and feedback channels. Everyone is encouraged to speak up, share ideas, and help shape the culture we build together.

We support colleague engagement by:

- Communicating frequently through local and Group leadership
- Using tools like engagement surveys and feedback loops
- Encouraging peer learning and cross-business collaboration
- Offering opportunities for internal mobility and career development
- Providing access to learning through the Purple Portal

If you're unsure where to find training or policies, speak with your manager or HR. All mandatory and role-specific training is available on the Purple Portal, our learning platform for onboarding, development, and compliance.

For support, contact your local HR team or Group HR (see Contacts).

## Doing Business Responsibly

### 3 Personal Integrity

Acting with integrity means doing the right thing – even when no one is watching. It’s about being honest, ethical, and fair in how we work, make decisions, and represent Diploma. Personal integrity is essential to protecting our people, performance, and reputation.

All colleagues are expected to:

- Follow the law and apply our Code in day-to-day decisions
- Avoid conflicts of interest and disclose them if they arise
- Use company assets and information responsibly
- Reject all forms of bribery, corruption, or unethical behaviour
- Raise concerns if something doesn’t feel right

You’re not expected to have all the answers, but you are expected to speak up and seek guidance. If in doubt, talk to your manager or refer to the Contacts section.

The following sub-sections provide guidance on common areas where integrity is critical.

#### 3.1 Conflicts of Interest

A conflict of interest arises when your personal interests interfere with – or even appear to interfere with – your ability to make fair, objective decisions at work. Even the perception of a conflict can undermine trust and damage our reputation.

You must always act in the best interests of the Group and avoid situations that create, or could create, a conflict. Some conflicts must be avoided entirely; others must be declared and managed transparently.

Examples of potential conflicts include:

- Having a second job or external role that overlaps with your Diploma responsibilities
- Having a financial interest in a supplier, customer or competitor
- Awarding business to a friend, family member or partner
- Using company assets or time for personal benefit
- Accepting gifts or benefits that could influence your decisions

If you are unsure whether something is a conflict, speak with your manager. Most situations can be managed if they are raised early and handled openly. You can also raise concerns confidentially through the Whistleblowing service (see Contacts).

All colleagues must declare any actual, potential, or perceived conflicts of interest and cooperate with any steps required to manage them.

For more information contact the Group Compliance Team (see Contacts).

## 3.2 Insider Trading and Share Dealing

Using confidential or inside information to trade shares—or sharing it with others—is illegal and strictly prohibited. Diploma complies fully with all legal and regulatory requirements and expects all colleagues to do the same.

You must not:

- Buy or sell Diploma shares while in possession of inside information
- Encourage others to deal in shares while you hold inside information
- Share inside or confidential information unless it's required for your role
- Trade in shares of another company if you have inside information about them

If you believe you may have access to inside information, report it to the Group Company Secretary. Do not share the information further unless instructed.

If you are classified as a Restricted Person, you must follow the Group Share Dealing Code. This includes:

- Seeking pre-clearance before trading
- Observing closed periods
- Reporting your transactions as required

Breaches of these rules may result in disciplinary action, fines, or criminal prosecution.

For more information, refer to the Group Share Dealing Policy and Code, or contact the Group Company Secretary (see Contacts).

## 3.3 Gifts, Hospitality and Entertainment

Gifts, hospitality, and entertainment (GH&E) can support business relationships - but only when they are appropriate, transparent, and never intended to influence decisions.

GH&E is permitted when it is:

- Clearly linked to a legitimate business purpose
- Reasonable in value, infrequent, and proportionate to the relationship
- Approved and recorded in line with the Group GH&E Policy
- Compliant with local laws and internal thresholds
- Attended by the host (in the case of hospitality or entertainment)

GH&E is not permitted if it:

- Involves government officials or politicians
- Occurs during or near contract negotiations or tenders
- Is lavish, excessive, or intended to create obligation
- Involves cash or cash equivalents (e.g. vouchers)
- Is frequent, or structured to avoid thresholds or disclosure

If you're unsure whether a gift or invitation is acceptable, ask your manager or raise a concern through the Whistleblowing service. For more information, refer to the Group GH&E Policy or contact the Group Finance Team (see Contacts).

### 3.4 Anti-Facilitation of Tax Evasion

Facilitating tax evasion is a criminal offence. Diploma has zero tolerance for any activity that supports or enables tax evasion, whether directly or through others.

You must never:

- Misclassify payments or documents to disguise their purpose
- Help someone hide income, avoid tax, or use false invoices
- Agree to use offshore accounts or inaccurate supplier details
- Ignore suspicious behaviour or warning signs
- Engage in or ignore conduct that could amount to 'cheating the public revenue' under the UK Failure to Prevent Fraud Act.

If you have any concerns or suspect that tax evasion may be occurring:

- Report it immediately to your Managing Director, Group Internal Audit, the Head of Tax, or the Legal Team
- Alternatively, report anonymously through the Whistleblowing service

Diploma pays its fair share of tax and does not engage in aggressive or artificial tax arrangements. All tax decisions are guided by legal compliance, transparency, and our core values.

Note: Facilitating tax evasion may also constitute fraud under the UK Failure to Prevent Fraud Act. HMRC expects all organisations to have adequate procedures in place to prevent both tax evasion and fraud.

Mandatory training is available on the Purple Portal and must be completed as required. For more information, refer to the Group Anti-Facilitation of Tax Evasion Policy or contact the Head of Tax (see Contacts).

## 4 Commercial Integrity

We conduct business fairly, honestly, and in compliance with all legal and regulatory requirements. Commercial integrity is essential to protecting trust - across customers, suppliers, partners, and regulators.

All colleagues must:

- Compete fairly and never engage in anti-competitive behaviour
- Comply with sanctions, anti-money laundering, and anti-bribery laws
- Maintain accurate business and financial records
- Follow approval and reporting processes
- Avoid any form of corruption, fraud, or misconduct

Integrity in our commercial dealings protects Diploma's reputation and ensures long-term success. The following sections outline key areas of risk and how to manage them responsibly.

If you're ever unsure how to act, seek advice from your manager or the relevant Group function (see Contacts), or report concerns through the Whistleblowing service.

## 4.1 Fair Competition and Anti-Trust

We compete fairly and never through illegal or anti-competitive practices. Competition and anti-trust laws protect customers, innovation, and the integrity of markets—and must be followed at all times.

You must never:

- Disclose to, discuss or agree with competitors on prices, discounts, tenders, or market allocation
- Share sensitive commercial information (e.g. pricing, margins, strategy, customer lists)
- Use third parties (e.g. agents or distributors) to coordinate with competitors
- Influence tenders or procurement processes unfairly
- Make misleading or disparaging statements about competitors

Watch for red flags such as:

- Receiving competitor pricing or strategy information – even informally
- “Off the record” conversations at trade shows or industry events
- Requests to align prices, discounts, or terms
- Sudden refusals to deal with certain customers without clear justification

Mandatory antitrust and competition law training is available on the Purple Portal and must be completed as required. If you're unsure whether an activity could breach competition laws, stop and seek advice from the Group Compliance Team (see Contacts) or report concerns through the Whistleblowing service.

## 4.2 Anti-Money Laundering

Money laundering is the process of hiding the criminal origin of funds to make them appear legitimate. It is illegal and poses serious legal and reputational risks. We are committed to doing business only with reputable customers, suppliers, and partners engaged in lawful activities. All colleagues must stay alert to suspicious behaviour and follow due diligence procedures.

You must not:

- Accept or process payments that are unusual, overly complex, or inconsistent with the transaction
- Ignore efforts to conceal ownership or identity
- Accept large cash payments or high-value transfers without approval
- Continue working with third parties who refuse to cooperate with checks

Red flags to watch for:

- Requests to split payments, overpay, or route funds through unrelated parties
- Incomplete or inconsistent customer or supplier records
- Reluctance to disclose beneficial ownership or account details
- Unusual refund or account adjustment patterns

If something doesn't feel right, raise it with your manager or the Group Compliance team. Concerns can also be reported through the Whistleblowing service.

## 4.3 Sanctions and Export Controls

We comply with all applicable trade and financial sanctions and export controls, including those imposed by the UK and other international authorities. Some regulations create restrictions on dealings with certain individuals, organisations, governments and jurisdictions, and some create limitations on the supply of specific products or services to certain end-use applications.

You must:

- Never knowingly work with or support sanctioned individuals or entities
- Stay alert to red flags in third-party relationships
- Seek advice if there is uncertainty about a transaction or counterparty
- Report any suspected breaches immediately
- Be aware of export controls which are applicable to products and services you trade in and seek advice from the Group Legal Team (see Contacts) if you need advice.

Failure to comply with sanctions laws can result in serious legal and reputational consequences for both individuals and the Group. For more information, refer to the Group Sanctions Policy or contact the Group Compliance Team (see Contacts). Concerns may also be raised through the Whistleblowing service.

## 4.4 Bribery and Corruption

Diploma has zero tolerance for bribery and corruption. We are committed to maintaining the highest standards of integrity and transparency in everything we do. Bribery includes:

- Offering, promising, giving, requesting, or receiving anything of value to improperly influence a decision
- Using gifts, hospitality, donations, or favours to gain or retain business advantage
- Involving third parties to carry out improper activities on your behalf

You must:

- Never offer, request, or accept bribes or facilitation payments
- Avoid even the appearance of improper influence, especially during tenders or negotiations
- Ensure all GH&E is appropriate, infrequent, and properly recorded (see Section 4.1.3)
- Complete due diligence before engaging third parties, especially in higher-risk markets
- Include anti-bribery clauses in relevant contracts
- Report any suspicious activity immediately

Facilitation payments, even if small or customary in some countries, are illegal under the UK Bribery Act and strictly prohibited—unless your safety is at risk. If so, comply only if absolutely necessary and report the incident right away.

Red flags include:

- Requests for cash without documentation
- Vague or inflated expense claims
- Unusual generosity during business decisions
- Reluctance to accept anti-bribery contract terms
- Payments to personal or offshore accounts

Mandatory anti-bribery and corruption training is available on the Purple Portal and must be completed as required. For more information, refer to the Group Anti-Bribery & Corruption Policy or contact the Group Compliance Team (see Contacts). Concerns can also be raised through the Whistleblowing service.

## 4.5 Fraud – Including Failure to Prevent Fraud

Fraud is any dishonest act intended to cause loss or gain, including misrepresentation, concealment, or abuse of position. It can be committed by employees, managers, or third parties acting on Diploma's behalf. We have zero tolerance for fraud and are committed to complying with the UK's Failure to Prevent Fraud Act, which requires organisations to implement reasonable procedures to prevent fraud by anyone associated with them.

### Red Flags to Watch For

Stay alert to signs that may indicate fraud or weak internal controls:

- Duplicate vendors, vague justifications, or unusual payment patterns
- Urgent changes to bank details without clear explanation
- Complex transactions with no obvious commercial purpose
- Avoidance of oversight, segregation of duties, or review
- Resistance to controls or excessive secrecy
- Pressure to meet unrealistic targets or delay bad news

### Your Responsibilities

All colleagues have a role in preventing fraud. You are expected to:

- Follow internal processes, controls, and approval requirements
- Declare any actual or potential conflicts of interest
- Never bypass system controls without proper authorisation
- Complete mandatory fraud awareness training
- Report concerns promptly – even if you're unsure

### Reasonable Procedures

Each Diploma business must implement proportionate, risk-based procedures to prevent fraud. These should reflect the nature and risk profile of the business and be applied consistently. Many are embedded in the Group's Minimum Controls Framework (MCF), which supports compliance with the UK's Failure to Prevent Fraud Act. Examples include:

- Documented review and approval for payments, contracts, journals, and new suppliers
- Clear delegation of authority and contract approval protocols
- Segregation of duties in high-risk processes (e.g. payments, procurement, financial reporting)
- Oversight of sales incentives, rebates, vendor onboarding, and customer credit decisions
- Due diligence on new suppliers, partners, and high-risk third parties
- Cycle counts and stock reconciliations in high-value inventory areas
- Periodic review of user access rights to finance, procurement, and HR systems
- Regular fraud awareness training for employees in sensitive or high-risk roles
- Promotion of the Whistleblowing service and protection for those who raise concerns

Local leadership is responsible for ensuring these controls are in place and enforced. Failure to implement reasonable procedures could expose the business and the Group to legal liability.

Common fraud risks are grouped as either causing company loss or benefiting the company, with corresponding controls outlined below:

| Types of Fraud                                                                                                                            | How it Could Be Prevented                                                                                                                                                |
|-------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Fraud Causing Company Loss</b>                                                                                                         |                                                                                                                                                                          |
| Expense fraud (false or inflated claims)                                                                                                  | Receipt requirements, policy limits, and random audits                                                                                                                   |
| Duplicate invoices                                                                                                                        | System-based duplicate detection and review before payment                                                                                                               |
| Fake invoices or vendors                                                                                                                  | Supplier due diligence and verification of contact and tax details                                                                                                       |
| Redirected payments via cyber fraud                                                                                                       | Independent callbacks to verify changes and dual verification processes                                                                                                  |
| Personal purchases using company accounts                                                                                                 | Clear usage policies, reconciliations, and manager oversight                                                                                                             |
| Failing to disclose conflicts of interest                                                                                                 | Declarations and restrictions on approval authority                                                                                                                      |
| Collusion with suppliers or customers to overbill                                                                                         | Independent contract reviews and <b>ethics training</b>                                                                                                                  |
| Ghost employees                                                                                                                           | Monthly payroll reconciliations and HR cross-checks                                                                                                                      |
| Misappropriation of inventory                                                                                                             | Stock audits, access restrictions, and physical controls (e.g. CCTV)                                                                                                     |
| Product substitution or false returns                                                                                                     | Cycle counts, return validation, and review of scrap/write-off trends                                                                                                    |
| Access rights abuse (excessive or unauthorised system access)                                                                             | Periodic access rights reviews in financial and HR systems                                                                                                               |
| Abuse of delegated authority                                                                                                              | Contract approval and review of exceptions to authorisation limits                                                                                                       |
| <b>Fraud Causing Company Gain</b>                                                                                                         |                                                                                                                                                                          |
| Capitalising costs that should be expensed                                                                                                | Capex review process and second-level approval of classifications                                                                                                        |
| Early or delayed revenue recognition                                                                                                      | Formal revenue recognition policy and finance oversight                                                                                                                  |
| Falsifying or inflating sales to meet targets                                                                                             | Independent sales validation and audit checks on bonus schemes                                                                                                           |
| Manipulation of provisions                                                                                                                | Requiring justification for large or late adjustments and periodic reviews                                                                                               |
| Concealing liabilities                                                                                                                    | Complete and timely accrual reporting and external audit review                                                                                                          |
| Undisclosed related party transactions                                                                                                    | Maintaining a related party register and requiring escalation and approval                                                                                               |
| Reconciliation manipulation or omission                                                                                                   | Independent review of key reconciliations (e.g. bank, suspense, inventory)                                                                                               |
| Inaccurate revenue or expense cut-off                                                                                                     | Structured cut-off testing during period close                                                                                                                           |
| Customer credit manipulation                                                                                                              | Credit checks, independent oversight of terms, and review of ageing reports                                                                                              |
| Unauthorised discounts or rebate abuse                                                                                                    | Approval of non-standard pricing and reconciliation of rebate claims                                                                                                     |
| Fraudulent customs declarations                                                                                                           | Cross-checking shipping records, random audits, and clear accountability                                                                                                 |
| Bank fraud or payment diversion                                                                                                           | Mandatory callbacks using known contacts and dual approval for account changes                                                                                           |
| Cheating the public revenue (e.g. facilitating tax evasion through misclassification, false invoices, or helping third parties avoid tax) | Staff training, transaction monitoring, due diligence on tax practices, whistleblowing protections, and cross-reference with the Anti-Facilitation of Tax Evasion Policy |

## Reporting Fraud

If you suspect or become aware of fraud, report it immediately. You can speak to your manager, local Finance lead, Internal Audit, or the Group Compliance team. Alternatively, you can raise concerns confidentially – and anonymously if you wish – through the Whistleblowing service.

You do not need proof to report a concern in good faith. All reports will be handled sensitively and investigated appropriately.

## 4.6 Charitable and Political Donations

Diploma supports charitable giving that aligns with our values and is managed transparently. All donations – whether monetary, in-kind, or through sponsorship – must be properly approved and documented. You must:

- Seek approval before making donations on behalf of the business
- Ensure all donations are lawful, transparent, and clearly recorded
- Never offer or make donations to influence a business outcome
- Never make political donations using company funds
- Vet charitable recipients where appropriate to manage regulatory and reputational risk

Even well-intentioned donations can raise concerns if not handled properly. If you're unsure whether a donation is appropriate, speak to your manager or contact the Group Compliance Team (see Contacts). Concerns can also be raised through the Whistleblowing service.

## 4.7 Responsible Tax Conduct

We are committed to paying our fair share of tax and managing our tax affairs with integrity and transparency.

Our approach to tax:

- Complies with all applicable tax laws in the countries where we operate
- Is based on commercial purpose, not aggressive or artificial arrangements
- Aligns with our values and long-term sustainability goals

We expect the same high standards from our businesses and partners. This includes:

- Accurate tax compliance, documentation, and reporting
- Transparent disclosures in line with our Group Tax Strategy
- Avoidance of schemes that could be considered tax evasion or abuse

For more information, refer to the Group Tax Strategy or contact the Head of Tax (see Contacts). You can also report concerns through the Whistleblowing service.

## 4.8 Accurate Records and Financial Responsibility

Accurate, complete, and timely records are essential for sound decision-making, legal compliance, and protecting our reputation. You must:

- Record all transactions truthfully, clearly, and in the correct accounts
- Follow internal approval processes and spending controls
- Never create or approve false, misleading, or incomplete records
- Retain documentation in line with Group policies
- Cooperate fully with audits, reviews, or investigations

This applies to all business activities – from financial reporting and contract documentation to expenses, operational data, and system entries. Falsifying records, concealing information, or misrepresenting data – financial or operational – can lead to disciplinary action and legal consequences.

For guidance or to raise concerns, contact your manager or the Group Finance Team (see Contacts). You can also use the Whistleblowing service.

## 5 Safeguarding Information and Systems

We each have a responsibility to protect Diploma's information, systems, and assets. Data and technology enable us to operate safely, serve customers, and make informed decisions – but if misused, lost, or accessed without authorisation, they can also expose us to risks.

This section outlines the behaviours and controls necessary to manage confidential information, protect personal data, and use IT systems responsibly.

### 5.1 Information Security

We must protect Diploma's systems and information from misuse, unauthorised access, and cyber threats. All businesses must:

- Comply with the Group Information Security Policy, which sets out the standards for safeguarding our systems and data.
- Follow the Group Incident Response Plan and any aligned local procedures in the event of a security incident.
- Due to its sensitive nature, details of the Incident Response Plan are confidential and available only to authorised personnel.

All colleagues must:

- Complete required training and follow security guidance
- Follow security guidance and report any incidents or threats promptly.

Refer to the Group Information Security Policy or contact the Group Integration Director for support (see Contacts).

### 5.2 Use of Technology and Cybersecurity

Our technology systems are essential for Diploma's operations. Protecting these systems and using them responsibly safeguards our data, reputation, and ability to serve customers. You must:

- Use company systems and devices only for authorised business purposes.
- Keep passwords secure – never share your login details.
- Avoid downloading unapproved software or storing business data on personal devices or cloud services.
- Report phishing attempts, cyber threats, or suspicious activity immediately.
- Follow local and Group procedures in the event of a data breach or cyberattack.

In serious incidents, escalate promptly following the Group Incident Response Plan. Each business must maintain a local plan aligned with Group standards.

Refer to the Group Information Security Policy and Group Incident Response Plan for guidance. For support, contact your manager or the Group Integration Director (see Contacts).

## 5.3 Use of Artificial Intelligence and Automation Tools

Artificial intelligence (AI) and automation can improve efficiency but must be used responsibly to avoid legal, ethical, and security risks. When using AI tools, you must:

- Never input confidential, personal or sensitive information into public or unauthorised AI tools
- Only use AI and automation tools that are approved by your business or IT team
- Ensure AI-generated content or decisions are reviewed by a human before being used or shared
- Comply with relevant policies on data privacy, intellectual property, and information security

Improper use of AI can result in data breaches, misinformation, or reputational harm. As AI technology and regulations evolve, Diploma may issue further guidance or restrictions. Always follow the latest Group or local instructions before using new tools or features.

For advice or approval, contact your local IT team or the Group Integration Director (see Contacts).

## 5.4 Intellectual Property

Diploma protects its intellectual property (IP) and respects the rights of others. You must:

- Keep company IP - including trademarks, product designs, and confidential information - secure and confidential
- Never use or share third-party IP (e.g. software, images, content) without permission or licence
- Report suspected misuse or infringement to the Group Legal Team promptly

Our IP is a valuable asset that supports our competitive advantage and reputation. Using it correctly helps protect both. For more information or to report concerns, contact the Group Compliance Team (see Contacts).

## 5.5 Data Privacy and Protection

We are committed to protecting the personal data of colleagues, customers, suppliers, and partners. All personal data must be handled lawfully, securely, and in line with applicable laws, including the UK GDPR. You must:

- Access or share personal data only when necessary for your role.
- Keep data accurate, up to date, and limited to what's needed.
- Store personal data securely and dispose of it properly when no longer required.
- Never transfer personal data using unapproved or unsecured methods.
- Report suspected data breaches immediately to your local compliance or Group Legal Team

Each business is responsible for local compliance and must follow Group policies and legal requirements. For support, contact your local compliance lead or the Group Compliance Team (see Contacts).

## 5.6 Responsible Communication and Social Media

How we communicate - internally and externally - reflects directly on Diploma's values and reputation. You must:

- Use email, messaging, and other tools professionally and respectfully
- Keep sensitive or confidential information secure in all communications
- Never use company systems for unlawful, offensive, or inappropriate content

- Only speak publicly on behalf of Diploma if authorised to do so
- Be cautious when posting or commenting on social media, even in a personal capacity

Never share confidential business information, make misleading or harmful statements, or post content that could damage Diploma's reputation. If you reference your role or employer online, make it clear that your views are personal and act responsibly.

If you're unsure, speak with your manager or the Group Investor Relations Team (see Contacts).

## 6 Health & Safety

We are committed to protecting the physical and mental health, safety, and wellbeing of all colleagues. Our ambition is to build a strong safety culture and achieve zero lost time incidents across the Group. Every business must comply with applicable safety laws and ensure safe working environments.

All businesses must:

- Maintain an up-to-date Health & Safety Policy and risk assessments
- Provide safe facilities, equipment, and working conditions
- Train employees on role-specific safety protocols
- Implement procedures for remote, off-site, or lone working
- Investigate and record incidents, near misses, and hazards via SML Connect
- Appoint a local Health & Safety Lead and hold regular safety reviews

All colleagues must:

- Follow safety rules and report unsafe conditions immediately
- Cooperate with inspections or incident reviews
- Take responsibility for personal and team safety
- Complete required training and ask for help if unsure

If you drive as part of your role, you must follow Diploma's driving safety procedures. This includes ensuring vehicles are roadworthy, taking regular breaks, never using a mobile device while driving, and complying with local driving laws.

Refer to the Group Health & Safety Policy and Driving Safety Policy for more information.

For support, contact your local Health & Safety Lead or the Group Sustainability Team (see Contacts).

### 6.1 Product and Service Safety

Delivering safe, high-quality products and services is a vital part of how we protect people, build trust, and operate responsibly. While our Health & Safety Policy focuses on the wellbeing of colleagues and contractors, we also have a duty to consider the safety of customers, end users, and the communities we serve.

We expect all businesses to take a proportionate, risk-based approach to managing product and service safety - integrated into day-to-day operations, not treated as an afterthought. This responsibility spans product design, sourcing, delivery, maintenance, and support.

Each business should:

- Assign clear accountability for product and service safety within local teams.
- Identify and assess safety risks across the product or service lifecycle.
- Provide training where safety responsibilities or technical risks are relevant to a role.
- Put in place appropriate checks (testing, approvals, or certification) before release or installation.
- Investigate incidents or customer complaints related to safety and act promptly to resolve issues.
- Monitor performance indicators (defects, complaints, returns) addressing trends or recurring risks.
- Test emergency procedures or recall protocols if failure could impact health or safety.
- Participate in relevant audits or third-party reviews where required.
- Be transparent with customers or regulators if serious safety concerns arise.
- Set improvement plans or targets where appropriate to reduce risk over time.

By embedding these principles, we help ensure our products and services are trusted, compliant, and safe to use – protecting people and strengthening our long-term reputation.

If you have concerns about product or service safety, raise them with your manager or through the Whistleblowing service.

## 6.2 Business Continuity and Crisis Preparedness

We are committed to protecting our people, operations, and customers by being prepared for disruptive events. Each business is expected to plan for, respond to, and recover from incidents that could interrupt critical activities – whether due to natural disasters, operational failures, supply chain disruption, or cyber incidents.

All businesses must:

- Maintain and regularly review Business Continuity Plans (BCPs) proportionate to their size and risk profile.
- Identify critical processes, people, and dependencies and ensure alternative arrangements are in place.
- Test plans periodically and ensure key colleagues know their roles during an incident.
- Escalate significant disruptions promptly to local leadership and Sector management, in line with local procedures.

Cyber incidents are addressed separately through our Information Security Policy and Incident Response Plan, which set out the required response and recovery processes. Business Continuity Plans should link to these to ensure coordinated response and recovery. For further guidance speak with your local leadership or Sector leadership.

## 7 Human Rights and Modern Slavery

We respect the dignity, rights, and freedoms of everyone we work with. Diploma is committed to upholding human rights, including the right to fair working conditions, freedom of association, and protection from forced or child labour.

All businesses must comply with applicable labour and human rights laws, and ensure that modern slavery, human trafficking, or exploitation do not occur in any part of our operations or supply chains.

All businesses must:

- Comply with applicable labour and human rights laws
- Monitor higher-risk geographies or sectors for modern slavery risks
- Conduct due diligence on suppliers and third parties
- Include contractual protections with suppliers, including rights to suspend or terminate where appropriate
- Support the Group's Modern Slavery Statement and escalation process

All suppliers and third parties must:

- Comply with labour and human rights standards
- Cooperate with due diligence, audits, or site visits
- Honour contractual terms, including the right to suspend or terminate relationships if concerns arise

All colleagues must:

- Be alert to poor working conditions or signs of coercion
- Raise concerns about suspected modern slavery or human rights abuse
- Complete relevant training or review guidance on modern slavery risks

Refer to the Group Modern Slavery Statement and Group Human Rights Policy for more detail.

For support, contact your manager or the Group Sustainability Team (see Contacts).

## 8 Working with Partners

We expect our suppliers, agents, contractors, and other partners to uphold high ethical, environmental, and social standards. The actions of third parties can affect Diploma's compliance, performance, and reputation, so we must choose and manage them carefully. All businesses should:

- Conduct proportionate due diligence on third parties before engagement
- Are encouraged to use contracts that include ethical, compliance, and termination clauses
- Monitor performance and behaviour, especially in higher-risk areas
- Escalate and act on concerns about third-party conduct

All suppliers and third parties are expected to:

- Comply with applicable laws and ethical standards
- Cooperate with oversight, audits, and investigations where required
- Acknowledge that failure to meet our expectations may result in suspension or termination of the relationship

All colleagues must:

- Select suppliers and partners based on merit, not personal connections
- Declare any conflicts of interest that could affect their judgment
- Report concerns about unethical or non-compliant behaviour by third parties

Refer to the Supplier Code of Conduct for more information. For support, contact your manager or the Group Sustainability Team (see Contacts).

## 9 Third Parties and Associated Entities

Third parties acting on behalf of Diploma – such as agents, distributors and consultants – must meet the same ethical, legal, and professional standards we expect of our businesses and colleagues. All businesses should:

- Conduct proportionate due diligence before engaging third parties, covering ownership, financials, legal history, and reputation
- Assess risks including bribery, fraud, sanctions, and data protection
- Ensure all third-party agreements include:
  - Anti-bribery and corruption clauses (including a ban on facilitation payments)
  - Audit rights and termination clauses
  - Provisions aligned with the third party's risk profile and local laws
- Monitor third-party conduct – especially in higher risk regions or sectors – and reassess risks when circumstances change
- Act on concerns, red flags, or non-compliance

All third parties are expected to:

- Operate in compliance with applicable laws and ethical standards
- Cooperate with oversight, audits, and investigations as required
- Honour contractual obligations – including Diploma's right to suspend or terminate relationships if standards are not met
- Manage environmental risks responsibly, including emissions, waste, and sourcing, as part of our sustainability commitments

All colleagues must:

- Select third parties based on merit and avoid personal conflicts of interest
- Declare any potential or actual conflicts that may affect judgment
- Report unethical or non-compliant behaviour by third parties

Refer to the Supplier Code of Conduct and Anti-Bribery & Corruption Policy for further detail. For guidance, contact the Group Sustainability Team or Group Compliance Team (see Contacts).

## Delivering for the Environment

Diploma is committed to reducing its environmental impact and embedding sustainability across all operations. Our goal is to achieve net zero greenhouse gas emissions by 2045, with interim targets of:

- 50% reduction in Scope 1 and 2 emissions by 2030
- 30% reduction in Scope 3 emissions by 2030 (from a 2022 baseline)

All businesses must:

- Comply with environmental laws and permit requirements
- Establish and maintain an Environmental Management System (EMS) suitable to their operations
- Reduce emissions, energy use, water consumption, and waste through operational improvements and innovation
- Apply circular economy principles and manage waste responsibly
- Handle hazardous materials safely and prevent pollution
- Work with suppliers and logistics partners committed to strong environmental practices
- Consider the environmental impact of business travel and, where possible, use virtual meetings or lower-emission travel options
- Assess and manage environmental risks and be prepared for incidents
- Monitor, report, and continuously improve environmental performance

Sustainability should be integrated into daily operations and long-term planning. All staff must be supported with tools and training to help achieve these goals.

Refer to the Group Environment Policy or contact the Group Sustainability Team for support (see Contacts).



## Our Policy Library

This Code is supported by a set of Group policies that provide detailed guidance on specific topics. These apply across all Diploma businesses and should be followed alongside this Code.

You can access the latest policies:

- On the Diploma Learning Management System (Purple Portal)
- Or via the Diploma website at <https://www.diplomapl.com/policies/>

### Policies on Website & Purple Portal:

- Code of Conduct
- Anti-Bribery & Corruption Policy
- Anti-Facilitation of Tax Evasion Policy
- Diversity, Equity & Inclusion Policy
- Environment Policy
- Gifts, Hospitality & Entertainment Policy
- Health & Safety Policy
- Human Rights Policy
- Information Security Policy
- Modern Slavery Act Statement
- Share Dealing Policy
- Supplier Code of Conduct
- Tax Strategy
- Whistleblowing Policy

### Policies on Purple Portal only:

- Health & Safety Policy – Driving
- Incident Response Plan
- Sanctions Policy
- Share Dealing Code
- Tax Policy
- Transfer Pricing Policy

## Contacts and Support

If you have questions about this Code, need help accessing training or policies, or want to raise a concern, support is available. Start by speaking with your line manager, local leadership team, or HR contact. For specific topics, use the contacts below:

|                                                     |                                                                                |
|-----------------------------------------------------|--------------------------------------------------------------------------------|
| Group CFO / Group Finance                           | <a href="mailto:Wilson.Ng@diplomapl.com">Wilson.Ng@diplomapl.com</a>           |
| Group CoSec & General Counsel                       | <a href="mailto:Anna.Lawrence@diplomapl.com">Anna.Lawrence@diplomapl.com</a>   |
| Group Compliance                                    | <a href="mailto:Compliance@diplomapl.com">Compliance@diplomapl.com</a>         |
| Group Legal                                         | <a href="mailto:Legal@diplomapl.com">Legal@diplomapl.com</a>                   |
| Group Integration Director / Head of Cyber Security | <a href="mailto:Carolyne.Dick@diplomapl.com">Carolyne.Dick@diplomapl.com</a>   |
| Group Risk, Audit & Assurance                       | <a href="mailto:Internal.Audit@diplomapl.com">Internal.Audit@diplomapl.com</a> |
| Group Tax                                           | <a href="mailto:Lauren.Orr@diplomapl.com">Lauren.Orr@diplomapl.com</a>         |
| Group HR                                            | <a href="mailto:HR@diplomapl.com">HR@diplomapl.com</a>                         |
| Group Sustainability                                | <a href="mailto:Sustainability@diplomapl.com">Sustainability@diplomapl.com</a> |
| Group Investor Relations                            | <a href="mailto:IR@diplomapl.com">IR@diplomapl.com</a>                         |

### Whistleblowing Service

If you're uncomfortable raising a concern through normal channels, use our Whistleblowing service, managed independently by Safecall.

You can contact Safecall 24/7:

- Website: [www.safecall.co.uk/file-a-report](http://www.safecall.co.uk/file-a-report)
- Email: [diploma@safecall.co.uk](mailto:diploma@safecall.co.uk)
- Phone: See your country's freephone number on the Safecall website

Reports are confidential. You may remain anonymous and do not need proof to raise a concern in good faith.

## Document Control

|                             |                       |
|-----------------------------|-----------------------|
| Policy owner:               | Group General Counsel |
| Published / effective from: | July 2026             |
| Review frequency:           | Annual                |
| Next review date:           | July 2027             |
| Version:                    | 8.0                   |

## Code of Conduct Declaration

All employees are responsible for upholding the standards and policies in this Code. This includes reading and understanding the Code, applying it in daily work, and seeking support when needed.

By signing this declaration, you confirm that you:

- Have received, read, and understood the Diploma Code of Conduct
- Will follow all relevant laws, policies, and procedures
- Will seek guidance if you are unsure about any requirement
- Will speak up if you witness or suspect unethical or illegal conduct
- Will complete all required compliance training
- Will respect local customs, provided they do not conflict with this Code or the law

Failure to comply may lead to disciplinary action, including dismissal, legal proceedings, or ending business relationships.

### Acknowledgement

Diploma Business: \_\_\_\_\_

Name: \_\_\_\_\_

Position: \_\_\_\_\_

Signature: \_\_\_\_\_

Date: \_\_\_\_\_