Idox Group International Business Conduct Policy

Contents

Our Commitment and Policies

Idox plc has introduced its International Business Conduct Policy to guide our accountable and responsible business practices, which applies to all companies within the Idox Group. The regulatory landscape is changing and Idox are committed at being at the forefront of corporate compliance.

About Idox

Idox Group is a leading supplier of digital software and services to a diverse customer base spanning both the UK and International markets. Spanning both the public and private sectors, Idox works across a range of industries and sectors – from central and local government to transport, health and social care and commercial organisations, to deliver smart technology that enhances services and improves productivity.

Responsibilities

Every employee has the responsibility to ask questions, seek guidance, report suspected violations, and express concerns about this policy and its related procedures. This International Business Conduct Policy is underpinned by detailed Group policies and procedures which assists employees in resolving questions and in reporting suspected violations. Managers are responsible for supporting implementation and monitoring compliance.

Ethical Business Conduct

The Idox Group conducts its business fairly, impartially, in an ethical and proper manner, and in full compliance with all laws and regulations. In conducting its business, integrity is the foundation of all company relationships, including those with customers, suppliers, communities and employees.

The highest standards of ethical business conduct are required of Group employees in line with their company responsibilities. Employees will not engage in conduct or activity that may raise questions to the Group's honesty, impartiality, or reputation or otherwise cause embarrassment to the Group. Conduct that is prohibited under this policy must not be carried out by anyone externally on behalf of the Group.

Anti-Corruption

Each member of the Group conducts its business in compliance with applicable anti-corruption laws and has instituted and maintained policies and procedures designed to promote and achieve compliance with such laws.

Bribery Act

The Board of the Group is committed to zero-tolerance in relation to any form of bribery and corruption and sees the Act as part of its overall corporate responsibility. The Group will work to identify and eliminate any form of bribery through a risk assessment process and ongoing monitoring and review. All employees are prohibited from soliciting, arranging or accepting bribes intended for the business and / or employee's benefit or that of the employee's family, associates or acquaintances. This policy extends to the Group's business dealings and transactions in the UK and abroad, whether on its own behalf or on behalf of any business managed or operated, wholly or in part, by any Group company.

This policy is supported by a detailed anti-bribery programme which will be regularly revised to capture changes in law, reputation demands and changes in the business.

Our policies on slavery and human trafficking

Idox Group is committed to acting ethically with integrity in all business relationships. The Group is responsible for ensuring employees are paid fairly and properly for their work, and developing systems and controls that safeguard against slavery and human trafficking taking place anywhere in our business or supply chains.

Constraints and Conflicts of Interest

As a publicly listed company with no links to the public sector other than commercial, the Group does not envisage any constraints on the provision of its services to the public sector. However, the Group understands that while working in a public sector environment there is the possibility of conflicts of interest being experienced by its employees, attempting to seek personal, family or community benefits as a result of opportunities presented to them during their work. The Group's policies of customer care, security and confidentiality protect the client to the extent that any breach of these policies is a clear breach of the employee's terms and conditions of employment and is thus an instantly dismissible offence.

Contracts

It is Idox Group policy that all customer contracts entered into by the Group require the customer to warrant that they have not received funding from any individual, entity, regime or government named on the sanctions lists of the UK and US governments which can be found at:

https://www.gov.uk/government/collections/financial-sanctions-regimespecific-consolidated-lists-and-releases (UK)

and

https://www.treasury.gov/resource-center/sanctions/Pages/default.aspx (USA)

Whistleblowing

1. About this Policy

1.1 We are committed to conducting our business with honesty and integrity and we expect all staff to maintain high standards. Any suspected wrongdoing should be reported as soon as possible.

1.2 This policy covers all employees, officers, consultants, contractors, volunteers, interns, casual workers and agency workers.

1.3 This policy does not form part of any employee's contract of employment and we may amend it at any time.

2. What is whistleblowing?

2.1 Whistleblowing is the reporting of suspected wrongdoing or dangers in relation to our activities. This includes bribery, facilitation of tax evasion, fraud or other criminal activity, miscarriages of justice, health and safety risks, damage to the environment and any breach of legal or professional obligations.

3. How to raise a concern?

3.1 We hope that in many cases you will be able to raise any concerns with your manager. However, where you prefer not to raise it with your manager for any reason, you should contact our Head of Corporate Services, Ruth Paterson or our CEO, David Meaden. Contact details are at the end of this policy.

3.2 We will arrange a meeting with you as soon as possible to discuss your concern. You may bring a colleague or union representative to any meetings under this policy. Your companion must respect the confidentiality of your disclosure and any subsequent investigation.

4. Confidentiality

4.1 We hope that staff will feel able to voice whistleblowing concerns openly under this policy. Completely anonymous disclosures are difficult to investigate. If you want to raise your concern confidentially, we will make every effort to keep your identity secret and only reveal it where necessary to those involved in investigating your concern.

5. External Disclosures

5.1 The aim of this policy is to provide an internal mechanism for reporting, investigating and remedying any wrongdoing in the workplace. In most cases you should not find it necessary to alert anyone externally.

5.2 The law recognises that in some circumstances it may be appropriate for you to report your concerns to an external body such as a regulator. We strongly encourage you to seek advice before reporting a concern to anyone external. Public Concern at Work operates a confidential helpline. Their contact details are at the end of this policy.

6. Protection and Support for Whistleblowers

6.1 We aim to encourage openness and will support whistleblowers who raise genuine concerns under this policy, even if they turn out to be mistaken.

6.2 Whistleblowers must not suffer any detrimental treatment as a result of raising a genuine concern. If you believe that you have suffered any such treatment, you should inform our Head of Corporate Services or CEO immediately. If the matter is not remedied you should raise it formally using our Grievance Procedure.

6.3 You must not threaten or retaliate against whistleblowers in any way. If you are involved in such conduct you may be subject to disciplinary action. In some cases the whistleblower could have a right to sue you personally for compensation in an employment tribunal.

6.4 However, if we conclude that a whistleblower has made false allegations maliciously, the whistleblower may be subject to disciplinary action.

6.5 UK employees: Public Concern at Work operates a confidential helpline. Their contact details are at the end of this policy.

7. Contacts

Head of Corporate Services: **Ruth Paterson**

Chief Executive: **David Meaden**

Public Concern at Work

(Independent whistleblowing charity - UK only)

www.pcaw.co.uk

whistle@pcaw.co.uk

Helpline 020 7404 6609

Anti-slavery and Human Trafficking

The Group is committed to acting ethically with integrity in all business relationships. The Group is responsible for ensuring employees are paid fairly and properly for their work and developing systems and controls that safeguard against slavery and human trafficking taking place anywhere in our business or supply chains.

The Group has adopted a risk-based approach to the assessment of our business and supply chain through our supply chain management policy, which has involved taking geographical, industry and market factors into account in order to identify categories of supply that may present a higher risk of modern slavery being present. We are focusing attention on suppliers in these category areas initially, although any resulting policy changes will extend to the whole business. Given the nature of what we do, we believe that there is a low risk of slavery or human trafficking having a connection with our business activities.

The main mitigations to ensure we are an anti-slavery business include:

- Ensuring our employees receive a fair wage.
- Supporting whistleblowing.
- Requiring compliance with our ethical conduct policy.
- Recruitment checks and supplier checks.

The Group see diversity as a strength and we are committed to respecting each individual's human rights and we provide equal opportunities to all qualified employees and applicants.

This statement is made pursuant to section 54(1) of the Modern Slavery Act 2015 and constitutes the Idox Group's slavery and human trafficking statement for the financial year ending 31st October 2018 and covers the following entities;

- Idox plc
- Idox Software Limited
- McLaren Software Limited

Occupational Health and Safety

By Management Review and staff training, the Group ensures that its performance relating to Occupational Health and Safety (OH&S) matters is subject to continual improvement.

The Group complies with all OH&S legislation and regulations applicable to its activities and to any other requirements to which the Group may subscribe, in particular in relation to the supply of specialist information management software solutions and services.

This OH&S Policy, held separately as part of the Health & Safety System, is maintained by regular review and is communicated to all of the Group's employees, suppliers and sub-contractors.

This OH&S Policy is made available to all interested parties including members of the general public.

This OH&S Policy is subject to regular Management Review in order to ensure that it remains relevant and appropriate to the Group's activities.

Equality and Diversity

Idox is committed to providing equal opportunities in all aspects of employment particularly recruitment, promotions and training.

Idox will provide equal opportunities to any employee or job applicant and will not discriminate either directly or indirectly on the grounds of age, race, colour, nationality, gender, sexual orientation, religion, marital status. Disabilities will be accommodated wherever practicable. Idox also affirms its commitment to treat part-time staff and contract workers as equitably as full-time staff, having regard to statutory obligations.

To meet these objectives Idox will ensure that:

- Selection criteria relating to job requirements are not discriminatory by asking for inappropriate qualifications or experience.
- Job descriptions and personnel specifications are not discriminatory.
- Job advertisements are not, without proper reason, confined only to certain publications, or worded in such a way as to exclude applicants either individually or of a particular group. Advertisements will carry a statement that the Group is an Equal Opportunities Employer.
- Every job is open equally to all applicants who meet the job requirements.
- Applications will be dealt with in accordance with appropriate procedure (See Code of Practice).
- Transfer, promotion and training are all open equally to all eligible employees and selection criteria do not exclude applicants from any group.
- Recruitment, selection and employment policies will be periodically reviewed and a detailed Code of Practice will be available to implement the Equal Opportunities Policy.

Code of Practice

The Group will not tolerate discrimination on any of the following grounds:

- By treating an individual on grounds of sex, colour, marital status, sexuality, race, nationality or ethnic or national origin, or membership or non-membership of a trade union, less favourably than others.
- By expecting an individual on the above grounds to comply with requirements for any reason whatsoever related to their employment, which are different to the requirements for others.
- By victimisation of an employee.
- By harassment of an employee.
- By imposing work that is more onerous on one employee than on others; or
- By any other act, or omission of an act, which has as its effect the disadvantaging of an employee or applicant against another, or others, purely on the above grounds.

It is the policy of the Group to ensure that entry into the company is determined solely by the application of objective criteria and individual merit. Equality will be accorded to applicants and employees without regard to disability, race, religion, gender, marital status, sexual orientation, colour, national or ethnic origin.

The objective of the Group is to employ individuals who are suitably qualified or who have the ability to develop the skills necessary to undertake the obligations imposed by the position they occupy.

Management Responsibility

The Chief Executive Officer has overall responsibility to ensure this policy is consistently applied and each manager has responsibility for the implementation of the policy in his or her area.

The Group has implemented the following measures to ensure that no discrimination or harassment occurs:

- Those with responsibility for staff are reminded that they may be held individually accountable for ensuring that no form of discrimination occurs in the recruitment, selection, promotion, training and discipline of these staff.
- Enquiries will be made into suspected cases of direct discrimination or acts of omission which lead to indirect discrimination. Any such practices will be stopped and disciplinary action may be taken against the individuals concerned.
- The Executive Management Team has the responsibility for ensuring that these policies on race, disability, gender, age, religion or belief, and sexual orientation are set out:
- In instructions to those concerned with recruitment, training, promotion, employee management in relation to disciplinary actions or employee grievances.
- In documents available to employees, recognised trade unions or other representative groups of employees.
- In recruitment advertisements or other literature.
- As information provided for employees and customers in accessible formats for disabled people.
- In relation to instructions or procedures for employees involved with service delivery, customer care and procurement of services and goods.
- In relation to sub-contractors used or employed.

Security and Confidentiality

The Idox Group is committed to the highest standards of information security, at present we are accredited to ISO 27001: 2013 standard. Underpinning this commitment is the Idox Group Information Security Policy which applies to all business functions and covers the information, information systems, networks, physical environment and people supporting these business functions.

The objective of Information Security is to ensure business continuity and minimise business damage by preventing and minimising the impact of security incidents. In particular, information assets must be protected in order to ensure:

- Confidentiality and protection against unauthorised disclosure.
- Integrity of information including protection against unauthorised or accidental modification.
- Availability as and when required in pursuance of the Organisation's business objectives.

The board of Idox has regular updates on the progress of Cyber Security, Data Integrity, Data Protection.

Work is ongoing across the Group in readiness for General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679). We have focus groups across the business ensuring that protection of data is at the heart of our products and our business processes.

Security and Confidentiality Policy

1.1 Confidentiality

The success of Idox is due, in part, to maintaining strict confidentiality with client information and between client projects.

Every employee has a responsibility to the company, its suppliers and customers to treat all information received as confidential.

It is Idox's policy to treat any client or supplier's information with sensitivity and not disclose this internally or externally unless the information already exists within the public domain.

It is the role of the Project Manager (PM) to ensure all staff involved in a project are briefed about any special security or confidentiality agreements. The PM should also remind staff about this policy at the beginning of each project and confirm they have read and understood its contents.

It is common practice to make use of Non-Disclosure Agreements, and these can take the form of a client's agreements or the Idox standard agreement.

1.2 Data Protection

1.2.1 Introduction

The Group has to collect and use certain types of information about clients, staff and general members of the public in order to conduct business. The information collected is about people who the Group has had contact with in the past and is likely to in the future. This includes current customers and suppliers, employees, prospective clients and others who the Group interacts with during the normal course of business.

In addition, in the provision of support to our customers we sometimes have access to their customers' personal data.

The Group also collects data to ensure compliance with other current and past relevant legislation.

This data ('Personal Data') will be collected, stored and used in full compliance with the Data Protection Act 1998 {The Act).

The Group recognises a moral duty to ensure that all such data is handled properly and confidentially at all times whether on paper or in an electronic format.

1.2.2 Principles

The Group will manage Personal Data in full compliance of the Act throughout the:

- Obtaining of Personal Data.
- Storage and security of Personal Data.
- Use of Personal Data, and
- Disposal/destruction of Personal Data not required for the conduct of business.

The Group will allow data subjects to have appropriate access to personal information relating to them.

The Group fully endorses and will adhere to the data protection principles set out in The Act, in particular, to the principles relating to personal information.

1. The Group shall process all Personal Data fairly and lawfully.
2. The Personal Data will only be obtained for one or more specified and lawful purposes and shall not be further processed for any other purpose which is incompatible with the normal legal conduct of the Group's business.
3. The Personal Data will be adequate, relevant and not excessive for the purpose(s) for which it is to be processed.
4. The Personal Data shall be accurate and kept up to date.
5. The Personal Data shall not be kept longer than is absolutely necessary or required by other current legislation.
6. The Group acknowledges the rights of individuals to whom the Personal Data relates, and ensures that these rights can be exercised in accordance with the Act.
7. The Group has put in place technical and organisational measures to ensure against unlawful or unauthorised processing of Personal Data and against accidental loss, destruction or damage to all data.
8. The Personal Data held by the Group will not be transferred to a country outside the European Economic Area.

1.2.3 How this will be achieved

The Company will follow and maintain strict safeguards and controls by:

- Nominating a 'Data Protection Officer' of sufficient seniority who is responsible for gathering and disseminating information and issues relating to information security, The Act and other related legislation. The nominated officer is David Meaden, Chief Executive responsible for all operational matters.

- All Senior Managers are responsible for communications and issues relating to information security, The Act, and other relevant legislation within their area of responsibility.

- The Group will ensure that all activities that relate to the processing of Personal Data have safeguards and controls in place to ensure full compliance with the Act.

- The Group ensures that all employees understand their individual responsibility relating to the requirements of The Act. Employees are provided with appropriate training, instruction and supervision so that duties are carried out effectively and consistently. Staff will only be given access to personal data that is appropriate for the effectively completion of their duties and tasks.

- The Group ensures that third parties (mainly suppliers) endorse the principles set out in the Act. In addition, third parties will only be provided with appropriate and minimal information for the duties/tasks to be undertaken.

- The Group will handle all requests for access to personal data courteously, promptly and appropriately. The Group will ensure that the data subject or an authorised representative has a legitimate right of access under the Act, that request is valid and the information provided is complete, clear and unambiguous. The Group will log all requests, the steps taken to validate the request and the information provided and/or withheld with reasons.

This Data Protection Policy will be reviewed regularly, in accordance with the Group's Information Security Management Policy, to ensure that the safeguards and controls in place are adequate, relevant and effective.

1.3 Security

Introduction

The Idox Group Information Security Policy applies to all business functions within the scope of the Information Security Management System and covers the information, information systems, networks, physical environment and people supporting these business functions. This document states the Information Security objectives and summarises the main points of the Information Security Policy.

Objective

The objective of Information Security is to ensure business continuity and minimise business damage by preventing and minimising the impact of security incidents. The Group ensures that third parties (mainly suppliers) endorse the principles set out in the Act. In addition, third parties will only be provided with appropriate and minimal information for the duties/tasks to be undertaken. In particular, information assets must be protected in order to ensure:

- Confidentiality i.e. protection against unauthorised disclosure.
- Integrity i.e. protection against unauthorised or accidental modification.
- Availability as and when required in pursuance of the Group's business objectives.

Responsibilities

The Board of Directors have approved the Information Security Policy.

1. Overall responsibility for Information Security rests with the Quality Manager.

2. Day-to-day responsibility for procedural matters, legal compliance including data protection, maintenance and updating of documentation, promotion of security awareness, liaison with external organisations, incident investigation, management reporting etc. rests with the Information Security Management System Manager.

3. Day-to-day responsibility for technical matters, including technical documentation, systems monitoring, technical incident investigation and liaison with technical contacts at external organisations, rests with the Head of Internal IT.

4. All employees or agents acting on the Group's behalf have a duty to safeguard assets, including locations, hardware, software, systems or information, in their care and to report any suspected breach in security to the Head of Internal IT or the Information System Management Manager without delay. Employees attending sites that are not occupied by the Group must ensure the security of the Group's data and access their systems by taking particular care of laptops, blackberries and/or similar computers and any information on paper or other media that they have in their possession.

5. The Information System Management Manager is responsible for drafting, maintaining and implementing this Security Policy and similarly related documents as detailed in Appendix II.

6. As with other considerations including Quality and Health & Safety, Information Security aspects are taken into account in all daily activities, processes, plans, projects, contracts and partnerships entered into by the Group.

7. The Organisation's employees are advised and trained on general and specific aspects of Information Security, according to the requirements of their function within the Organisation. The

Contract of Employment includes a condition covering confidentiality regarding the Organisation's business.

8. The Group's employees are advised and trained on general and specific aspects of Information Security, according to the requirements of their function within the Group. The Contract of Employment includes a condition covering confidentiality regarding the Group's business.

9. Adherence to Information Security procedures as set out in the Group's various policies and guideline documents is the contractual duty of all employees and a clause to this effect is set out in the Group's contracts of employment.

10. Copies of the Information Security Management Manual are made available to all of the Group's employees.

11. Breach of the Information Security policies and procedures by the Group's employees may result in disciplinary action, including dismissal.

12. In view of the Group's position as a trusted provider of document, content and information management systems that allow the delivery of information to the citizen and clients across the internet, extranet or intranet, particular care is taken in all procedures and by all employees to safeguard the Information Security of its service users and/or clients.

13. Agreements of Mutual Non-disclosure/Confidentiality are entered into as appropriate with third party Companies.

14. All statutory and regulatory requirements are met and regularly monitored for changes.

15. A Business Continuity Plan is in place. This is maintained, tested and subjected to regular review by the Information System Management Manager.

16. Further policies and procedures such as those for access, acceptable use of e-mail and the internet, virus protection, backups, passwords, systems monitoring etc. are in place, maintained and are regularly reviewed by the Information System Management Manager and the Head of Internal IT or an appointed representative, as appropriate.

17. This Information Security Policy is regularly reviewed and may be amended in order to ensure its continuing viability, applicability and legal compliance, and with a view to achieving continual improvement in the Information Security Systems.

Environmental Safety

1. Environmental Policy Objectives

Idox group companies (the 'Group') recognises the importance of environmental protection and is committed to operating its business responsibly and in compliance with all legal requirements relating to the development and sale of products for document, content and information management. It is the Group's declared policy to operate with and to maintain good relations with all regulatory bodies.

In support of this policy, the Group operates an Environmental Management System, the scope of which is set out below.

It is the Group's objective to carry out all measures reasonably and practicable to meet, exceed or develop all necessary or desirable requirements and to continually improve environmental performance through the implementation of the following:

a. Assess and regularly re-assess the environmental effects of the Group's activities.
b. Training of employees in environmental issues.
c. Minimise the production of waste.
d. Minimise material wastage.
e. Minimise energy wastage.
f. Promote the use of recyclable and renewable materials.
g. Reduce and/or limit the production of pollutants to water, land and air.
h. Control noise emissions from operations.
i. Minimise the risk to the general public and employees from operations and activities undertaken by the Group.

This policy is communicated to all employees, suppliers and sub-contractors and is made available to the public.

The person responsible for implementation of this policy is the Chief Executive Officer of Idox plc.

2. Environmental (Purchasing) Policy

The Group operates an approved supplier list for all of its purchases. When selecting a supplier the Group will give preference to a supplier that can demonstrate a sound environmental policy of its own, preferably supported by ISO 14001 accreditation.

In addition, when selecting a product for purchase, the Group applies the following criteria:

2.1.1 Resource Use and Recycling

- Does production/extraction of the product cause ecological damage, such as loss of habitats or damage to threatened species? Are there alternatives?
- Is this a remanufactured product?
- Can the product be re-used, refilled, recharged or reconditioned to extend its life?
- Can the item be easily upgraded by adding or replacing a part?
- Does the product have a recycled content? What percentage?
- Is the product accredited with a recognised environmental standard?
- Can the product be recycled easily (in the workplace and/or local community)?

2.1.2 Hazardous Content

- Is the product or are its components hazardous to humans and/or the wider environment? If yes, what are the health and safety implications and disposal requirements? Are there any non-hazardous alternatives available?
- Are technical data sheets available?

2.1.3 Energy

- Does the item use energy (e.g. electrical appliances, equipment, machinery, space heating or vehicles)?
- If so, is the item as energy efficient as the alternatives?
- Does the item have energy consumption data for all operation modes?

2.1.4 Packaging

- Can product packaging be reduced or eliminated?
- Is packaging made of recycled material(s)?
- Can packaging be re-used, recycled or returned?

2.1.5 Transportation

- Is the product locally manufactured and/or locally supplied?
- Does the supplier have a Green Transport Plan for their operations?

2.1.6 Supplier Environmental reporting

- Does the supplier have a company Environmental Management System?
- Does the supplier report on their environmental performance against set targets?

3. Environmental Management System Accreditation

Idox Software Ltd is accredited to BS EN ISO 14001:2015 which encompasses this Policy and the Environmental Management System.

Signed:

David Meaden

Chief Executive Officer

Date: 05.08.2020

Inside Information and Share Dealing

In the course of your employment with the Idox Group, you may become aware of information about Idox Group or other companies that has not been made public. The use or disclosure of such non-public or "inside" information about Idox or another company for your financial or other benefit is not only unethical, but also it may be a violation of the Market Abuse Regulation applicable in the UK and across the EU. These laws make it unlawful for any person who has "material" non-public information about a company to trade the shares of that company. Violation of such laws may result in civil and criminal penalties, including fines and jail sentences. The Idox Group will not tolerate the improper use of inside information. These prohibitions also apply anywhere in the world where we do business. All employees are to comply with the Idox Group Share Dealing Policy.

Idox Group Share Dealing Policy (Adopted on 1 July 2016)

This policy applies to all directors and employees of Idox plc (the Company) and its subsidiaries. It has been designed to ensure that you do not misuse, or place yourself under suspicion of misusing, information about the Group which you have and which is not public.

1. You must not deal in any securities of the Group if you are in possession of inside information about the Group. You also must not recommend or encourage someone else to deal in the Group's securities at that time – even if you will not profit from such dealing.

2. You must not disclose any confidential information about the Group (including any inside information) except where you are required to do so as part of your employment or duties. This means that you should not share the Group's confidential information with family, friends or business acquaintances.

3. You may, from time to time, be given access to inside information about another group of companies (for example, one of the Group's customers or suppliers). You must not deal in the securities of that group or companies at those times.

4. The Group also operates a Dealing Code which applies to the Company's directors and to employees who are able to access restricted information about the Group (for example, employees who are involved in the preparation of the Group's financial reports and those working on other sensitive matters). You will be told if you are required to comply with the Dealing Code. Directors and employees who are required to comply with the Dealing Code must also comply with this policy.

5. The Group also operates a Dealing Code which applies to the Company's directors and to employees who are able to access restricted information about the Group (for example, employees who are involved in the preparation of the Group's financial reports and those working on other sensitive matters). You will be told if you are required to comply with the Dealing Code. Directors and employees who are required to comply with the Dealing Code must also comply with this policy.

6. Failure to comply with this policy may result in internal disciplinary action. It may also mean that you have committed a civil and/or criminal offence.

7. If you have any questions about this policy, or if you are not sure whether you can deal in securities at any particular time, please contact the Company Secretary.

- Idox Group Securities Dealing Code for Restricted Persons

http://investors.idoxgroup.com/downloads/CorpGovernance/Idox-Group- Securities-Dealing-Code-for-Restricted-Persons.pdf

- Idox Group Securities Dealing Procedures Manual

http://investors.idoxgroup.com/downloads/CorpGovernance/Idox-Group- Securities-Dealing-Procedures-Manual.pdf

Contact us

Idox Software Ltd

Second Floor, 1310 Waterside

Arlington Business Park

Theale RG7 4SA

T: +44 (0) 333 011 1200

E: info@idoxgroup.com

www.idoxgroup.com