Code of Conduct

Consolidated Ethical Policies

Published 27th April 2021

Don-Bur (Bodies & Trailers) Limited, Registered Office: Mossfield Road, Adderley Green, Longton, Stoke-on-Trent, Staffordshire, ST3 5BW. Registered in England No: 1571914. VAT Registration No. GB319377927

Tel: 01782 599 666 | www.donbur.co.uk

Contents

1 Introduction

Responsible business practice is part of our heritage and is one of the key foundations for company health, trust and productivity. Responsible business conduct is also just simply good for business.

Our reputation is affected by the way employees act inside the company and with external parties. That reputation ultimately affects our growth and profitability. It is therefore important that we act according to the highest ethical standards and with integrity in order to earn and maintain the trust of our customers, stakeholders and the communities in which we operate, as well as our colleagues.

The responsibility to practice those standards belongs to all of us. Simply having a Code of Conduct is not sufficient and how we carry it out it is just as important as what we carry out. It is also important that everyone working at, or with, Don-Bur is comfortable raising questions or concerns about ethical issues. We support a culture of transparency, integrity and accountability.

To guide and promote good governance and ethical behaviour across our group, we maintain a series of policies. These guide our actions and those of our employees, suppliers and partners.

2 Principles of Social Responsibility

2.1 Fair working conditions

In recognition of the importance of providing fair working conditions, Don-Bur respects people and recognises fundamental human rights and expects people working and employed by Don-Bur ("Associates") to act in the same way.

2.1.1 Non-discrimination and Non-harassment

Don-Bur does not tolerate acts of discrimination or harassment. In particular, Don-Bur does not:
(1) unlawfully discriminate against anyone based on, for example, race, sex, age, sexual orientation, pregnancy, political affiliation, union membership, marital status, nationality, ethnic background, religion, or disability; or,
(2) violate a person's dignity by engaging in harassment or abuse (on any grounds or in any form), corporal punishment, mental or physical coercion or threat of any such treatment.

2.1.2 Fair and Lawful Labour Practices

Don-Bur strives to comply with all local laws and regulations, instructions of competent authorities or appropriate local industry practices in relation to working conditions including hours, wages and benefits (including minimum wages) and overtime hours.

2.1.3 Freedom of Association

Don-Bur respects the rights of employees to associate freely with others, join or not join labour unions, seek representation and join workers' councils in accordance with local laws and regulations.

2.1.4 Child and Forced Labour

Don-Bur does not tolerate or engage in illegal labour practices. In particular Don-Bur does not:
(1) use forced labour or involuntary prison labour;
(2) require Associates to hand over government-issued identification, passports or work permits to Don-Bur as a condition of employment (except temporary hand over for identification confirmation or government formalities);
(3) knowingly employ any persons below the age for completing compulsory schooling in accordance with local laws;
(4) knowingly employ persons under 15 years old (or 14 where the law of the country permits); or
(5) assign Associates under the age of 18 to work that is likely to jeopardize their health or safety.

Anti-Slavery Policy

2.1.5 Clearly defined disciplinary policies

Don-Bur shall clearly define disciplinary policies and procedures and communicate these policies and procedures to its employees.

2.1.6 Whistleblowing system

Don-Bur has established a whistleblowing policy and system and encourages Associates to report any violations of these principles, other company policies, local laws and regulations. Don-Bur does not authorise Associates to retaliate against persons for making a good faith report of a violation and, where appropriate and if permitted by local laws, shall ensure the anonymity of any whistle-blowers.

3 General Ethical and Respectable Business Practices

Don-Bur will act with the highest integrity and ethics in all aspects of our activities.

3.1 Fair Dealing

Don-Bur will comply with the anti-trust and competition laws of the countries and regions which apply to our operation and will not engage in any acts which will restrict or distort free and fair competition.

In purchasing goods and services, Don-Bur will select suppliers impartially and upon fair conditions.

3.2 Proper Advertising

Don-Bur shall uphold and comply with applicable standards of advertising and Don-Bur will refrain from knowingly using any misleading or inaccurate advertising.

3.3 Improper Advantage

Don-Bur shall not engage in any form of corruption, extortion or embezzlement. Bribes or other means of obtaining undue or improper advantage are not to be offered or accepted.

3.4 Reporting and Recording Accurate Corporate Information

Don-Bur shall record and report all necessary information including accounting records promptly and accurately, and retain them properly.

Don-Bur shall make accurate and timely disclosure of financial status and information on business operations to shareholders, investors and applicable capital markets to facilitate informed investment decisions in accordance with applicable laws and regulations.

Moreover, Don-Bur shall require Associates to ensure that statements of a personal nature appearing in newspapers or magazines, and on radio, television, video or via the internet will not give the appearance of speaking or acting on Don-Bur's behalf.

3.5 Information Management

Don-Bur has rigorous information management systems and ensures that Associates will not unlawfully disclose confidential information relating to Don-Bur companies, other organisations or our customers to third parties without consent.

3.6 Protection of Personal Information

Don-Bur respects the privacy of our customers, business contacts and Associates and has developed safeguards designed to limit access to their personal information in accordance with local privacy laws. Don-Bur safeguards private information, including personal data, lists of our customers and employees and does not authorise our Associates to share private information, unless it is done in accordance with local data protection laws and our applicable privacy policies and GDPR protocols or otherwise with permission, as appropriate.

3.7 Protection of Intellectual Property Rights

Don-Bur shall endeavour to secure, maintain, and expand Don-Bur's intellectual property rights (including but not limited to patent rights, trademark rights and copyrights) and Don-Bur will respect the intellectual property rights of third parties. Don-Bur and Associates shall not intentionally infringe the intellectual property rights of others.

3.8 Management System to Implement these Principles

Don-Bur will establish a management system to implement these Principles as follows:
(1) each Don-Bur Group company shall implement its own code of conduct which, together with other company rules, satisfies the standard set by these Principles and require its Associates to comply with such code;
(2) each Don-Bur Group company shall, according to its organisation, clarify the department responsible for implementation of its code of conduct;
(3) each Don-Bur Group company shall give regular training to its employees with respect to compliance with its code of conduct;
(4) each Don-Bur Group company shall perform periodic auditing to ensure conformity with these Principles; and,
(5) each Don-Bur Group company shall correct in a timely fashion any deficiencies identified by periodic audits.
The senior management at Don-Bur (Bodies & Trailers) Ltd shall be responsible for ensuring implementation of these Principles by each company of Don-Bur and the management systems as well as reviewing the status of the management system on a regular basis.

4 Corruption & Anti-Bribery Policy

4.1 Background

This policy applies to all members of Don-Bur. For the purposes of this policy, the term "member" means all staff including permanent, fixed term, and temporary staff.

All employees will be made aware of this policy on induction to the company. All Don-Bur employees and associates are required to act honestly, responsibly and with integrity and to safeguard the Company by operating

All contractors and agents acting for or on behalf of the Company should be made aware of this policy, particularly during any procurement process. Reasonable due diligence must be carried out to ensure they are not acting in a way contrary to our policy or procedure.

Third parties acting for us are expected to take appropriate action should it be suspected or discovered that fraudulent activity or bribery is evident.

Any employee who is found to be in breach of this policy will be subject to disciplinary procedures. Members are reminded that fraud and bribery are also criminal offences. Don-Bur also reserves the right to seek redress via civil proceedings against individuals whose fraudulent acts or omissions have resulted in financial loss to the Company.

This policy has been developed to comply with the provisions of the Bribery Act 2010.

4.2 Anti-Bribery Policy

Don-Bur does not participate in any form of bribery, fraud or corruption. We are committed to safeguard the proper use of Company finances and resources and operate a zero-tolerance policy in respect of bribery.

This means that people acting or working for us must never:

- Offer or make a bribe or solicit business by offering a bribe, unauthorised payment or inducement of any kind to anyone;
- Accept any kind of bribe, unauthorised payment or inducement that would not be lawful or authorised by us in the normal course of events.

4.2.1 Definitions

Corruption is the misuse of public office or power for private gain, or misuse of private power in relation to business outside the realm of government.

Bribery is the means of offering, promising, giving, requesting or accepting anything of value (for example, money, gifts, hospitality, favours, information, job opportunities or any other benefit or advantage) with the purpose of improperly obtaining an advantage.

The Bribery Act 2010 introduced four offences:

1. Offering a bribe (applies to both individuals and corporations);
2. Receiving a bribe (applies to both individuals and corporations);
3. Bribing a foreign public official (applies to both individuals and corporations);
4. Failing to prevent bribery (applies to corporations only).

4.2.2 When and how to report

The prevention, detection and reporting of bribery is the responsibility of all employees. If you are in a situation and unsure whether you are being offered a bribe or are concerned your conduct could suggest you are offering a bribe, the following must be considered:

- Have I consulted the right people?
- Could I explain my actions/decision to others and feel comfortable?
- Is it consistent with the Company's behavior and way of doing business?
- Is this legal?

If the answer to any of the following questions is "no" or "don't know" then stop and seek advice from the Company Secretary before acting.

Central to the operation of this policy is transparency in our business

dealings. It is therefore imperative if you receive an offer that may be

interpreted as a bribe, a payment or inducement this must be declared to the Company.

4.2.3 The consequences of bribery

Bribery is a serious matter and a criminal offence. An individual who breaches the Bribery Act risks:

- disciplinary investigation/being dismissed from their post;
- a criminal investigation resulting in a possible prosecution and a possible custodial sentence (which could result in a custodial sentence of up to 10 years and/or an unlimited fine);
- if you benefited financially, you risk prosecutions/convictions under money laundering laws and the Proceeds of Crime Act 2002;
- if you committed the act abroad you may also be subject to that country's laws.

As a company we risk, amongst other sanctions:

- an unlimited fine;
- irreparable reputational damage.

4.3 Hospitality and Gifts

Hospitality, entertainment and gifts that are frequent, lavish or extravagant will be perceived to have influenced the recipient.

This policy is not designed to prevent staff from receiving hospitality or gifts but to set out clear guidance to avoid doubt and confusion. Hospitality and gifts should be both sensible and proportionate to the circumstances. You have an obligation to disclose the receipt of any gift/hospitality to the Company in the course of your duties.

4.3.1 Giving Gifts

An employee may not directly, or through others, offer or give any gift, hospitality, money or other thing of value to any official, employee or representative of any supplier, customer or any other organisation which if doing so could reasonably give the appearance of influencing the organisation's relationship with the Company. To do so could seriously damage our reputation and you may also be breaking the law.

Employees (if empowered to do so) may do the following:

- Give a gift of nominal value, such as stationery, pens etc., where appropriate;
- Provide meals and other entertainment at external venues provided the expenses are reasonable and approval has been given by a Director.
- Provide meals and overnight accommodation where this is reasonable and in the normal course of Company business or events.

4.3.2 Receiving Gifts and Hospitality

Staff must not accept any gifts or hospitality, regardless of value, which may influence or be perceived to be seen to influence situations such as awarding of contracts, use of Company assets or to benefit another personally or professionally.

In the course of duties, staff may find themselves in a position where they are in receipt of gifts/hospitality. In accordance with the Bribery Act 2010, received hospitality and gifts must be both sensible and proportionate

4.3.3 Acceptable gifts or hospitality

Unless you have been instructed otherwise, staff may accept the following:

- Gifts of nominal value, such as advertising gifts (such as pens, stationary etc.), when it is customarily offered to others having a similar relationship with that individual or organisation;

- Customary meals or entertainment provided that the expenses are reasonable and the meal/entertainment is within the usual course of business.

Any other gift which does not fall within the above criteria should be politely declined.

There may be occasions where you have no warning that a gift or hospitality will be offered. There are some circumstances, where to refuse a gift could cause offence to your hosts. In these circumstances, the gift/hospitality can be accepted but must be disclosed on your return.

4.3.4 Disclosing hospitality and gifts.

If you are offered hospitality or gifts, the following procedure should be used.

You must:

Disclose the offer to your line manager prior to the event and they will provide you with authorisation to attend.

In the event of any doubt about any probity of such hospitality, advice should be sought from the Company Secretary.

In exceptional circumstances a gift that is personal in nature may be retained subject to approval by the Company.

4.4 Conflict of Interest

A conflict of interest is a situation where financial or other considerations could influence, or appear to influence, an employee's professional judgement, performance or decisions. Any personal relationship that affects a person's decision-making abilities or their ability to carry out their duties objectively is also a conflict of interest.

4.4.1 Obligation to report

Employees can take part in activities outside their normal jobs but are required to disclose situations to their manager that could potentially rise to become a conflict of interest. The disclosure allows finding a mutual solution to handle the situation. There is also an obligation to disclose if a relative or friend has an engagement in a company that has a business relationship with Don-Bur and his or her activities for that company could somehow be linked to your duties at Don-Bur. A formal report should be submitted if you, have any financial engagement as defined in the policy and it is, or could appear to be a conflict of interest.

4.5 Measures to Prevent Corruption

Internal audits are performed and stored to spot any potential frauds in high-risk areas. Goods are tracked from order (random selection) to ensure they physically arrive and are costed onto legitimate contracts in progress.

All expenses are signed by a Director so that there is full understanding and the highest authorisation level for items being purchased in this way.

The staff induction process includes Corruption & Bribery and Whistleblowing policies; all of which are available separately.

4.6 Whistleblowing Policy

The aim of the policy is to help employees to raise any serious concerns they may have about colleagues with confidence and without having to worry about being victimised or disadvantaged in any way as a result.

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

Employees should not hesitate to “speak up” or “blow the whistle” if they believe malpractice may be occurring.

Individuals may be anxious that, by reporting genuine whistleblowing concerns, their actions may leave them vulnerable. It is important to emphasise that Don—Bur as an organisation will not tolerate the victimisation, intimidation or penalisation of anyone raising a genuine concern, anyone involved in the subsequent investigation or anyone acting as a witness.

Concerns should, in the first instance, be taken to an appropriate Director. All concerns will be investigated and dealt with as appropriate. The Director involved will ensure that the shareholders are informed and are involved as appropriate. The staff member who raised the concern or issue will be informed of the outcome of the investigations and what, if any, action has been taken.

If the staff member is unhappy about the speed, conduct or outcome of the investigation, they should put their concerns in writing to the Chairman.

Under this policy the disclosure must be made to an appropriate Director. The person making the claim must have reasonable belief that wrongdoing is being or is about to be committed. There must be reasonable belief that for it to be substantially true and that the disclosure is in the public interest.

The person making the claim should not collect the information to support the allegations improperly.

Where it is found that the whistle—blower makes an allegation:

Maliciously, or does not act in the public interest

Without having reasonable grounds for believing it to be substantially true

Collects the information to support the allegations improperly

Makes an allegation for personal or 3rd party gain

They will be subject to formal disciplinary action, up to and including dismissal and in some cases may be subject to criminal investigation where illegality has occurred in order to achieve those aims.

5 Anti-Slavery Policy

This statement is made on behalf of the board of Don-Bur (Bodies & Trailers) Limited with regards to the Modern Slavery Act 2015. The Act requires large employers to be transparent about their efforts to eradicate Slavery and Human Trafficking within their supply chain.

We have been a supplier of Bodies and Trailers to the transport industry for 35 years, also providing Repairs and Services to operators within the industry. Our company is based at three different sites within Stoke-on-Trent.

5.1 March 2021

Over the last 12 months the whole business focus shifted to survival with the ravaging effects of the Covid 19 pandemic.

The bulk of our workforce were on furlough leave from March 2020 for several months, with a ban on unnecessary travelling in force thereafter. Our plans to visit suppliers were therefore stopped in their tracks, but will resume once a more normal way of working resumes.

5.2 March 2019

We have, since our last statement, continued to develop our commitment to improving practices that ensure there is no slavery or human trafficking in our supply chains or any other part of our business. The products we sell are sourced mainly from the UK, but are manufactured in many different countries, and include many well-known branded products. We aim to ensure that these values are upheld across all of our supply chain.

To achieve this, we are assessing areas of our business where there could be potential risks of modern slavery within our supply chain. Over the last year we have begun to develop and implement systems and controls to review and monitor compliance with our policy.

5.2.1 Supplier Correspondence

We purchase products from UK and European-based supplier companies, many of whom are part of larger global organisations. These organisations acknowledge and generally publish their commitment to anti-slavery practices.

We have presented our major and high risk suppliers with a copy of our Anti-Slavery policy, with the expectation that their own policies and the policies of their own suppliers meet our same high standard. We are now actively corresponding with our major suppliers, requesting

their anti-slavery (and ethical) policies and statements and seeking positive confirmation of their commitment to compliance with our standards.

We will assess any instances of non-compliance if and when they arise, and take the appropriate action to remedy such non-compliance. If we find serious breaches to our core policy our suppliers have been informed that we will instantly seek an alternative supply route.

5.2.2 Supplier Visits

Our materials are sourced from manufacturers in several countries around the globe and are often manufactured to our own specification and design. As at 31 March 2019 we had active relationships with circa 250 core suppliers, predominantly in the UK and Europe.

To help ensure that we aren't involved in modern slavery or the infringement of human rights in any way we have started to conduct our own independent inspections of third-party facilities involved in the manufacture of products that we use. During these inspections we will carry out extensive checks and produce written 'factory inspection' reports.

We have begun documenting such supplier checks and have recently visited key suppliers as far away as Asia to ensure our standards are met.

Checks will include:

- Working environment - Ventilation, lighting, cleanliness, temperature
- Working hours of factory employees
- Machinery & equipment standards and guards
- Safety equipment including firefighting equipment and first aid kits
- PPE & training
- Emergency exits & signage
- Staff facilities
- Factory certification

5.3 March 2018

Our Supply chains are predominantly based in the UK and we are committed to ensuring that there is no modern slavery or human trafficking within our supply chains or in any part of our business.

We are committed to acting ethically and with integrity in all our business relationships and to implementing and enforcing effective systems and controls to ensure slavery and human trafficking is not taking place anywhere in our supply chains.

As part of our initiative to identify and mitigate risk, we are contacting our supplier base in relation to slavery and human trafficking. We will make our best efforts to ensure that we only work with suppliers who acknowledge their obligations towards modern slavery.

The system we are putting in place will:

- Identify and assess potential risk areas in our supply chains.
- Mitigate the risk of slavery and human trafficking occurring in our supply chains.
- Monitor risk areas in our supply chains.

6 Supply Chain Code of Conduct

Don- Bur is fully committed to doing things the right way. This means being true to our values and standards, working with integrity and supporting each other along the way right across the supply chain.

6.1 Impact on the Supply Chain

Don-Bur sources products and services for its distribution and sales operations from several countries around the world. We recognise that there are local and national differences in standards in relation to many aspects of the manufacturing and wider business environment. However, we also recognise that there are a number of minimum standards that must be achieved by all. Don-Bur has a supply chain policy and expects all Don-Bur businesses and employees to comply with it.

6.2 Policy Commitments – Don-Bur's Requirement of Suppliers

It is Don-Bur's policy only to work with suppliers that meet or exceed the following requirements:

- Employees of our suppliers shall work hours that comply with national laws.
- All our suppliers shall take responsibility to protect the health and safety of their employees. Suppliers must control hazards and take the best precautions against accident and occupational diseases.
- No children are to be employed by Don-Bur's suppliers. We support the long-term objective to eliminate child labour consistent with the United Nations Convention on the Rights of the Child.
- Suppliers will comply with all appropriate local legislation.
- All our suppliers shall protect the environment to minimise environmental pollution and make continuous improvements in environmental protection.
- All suppliers to provide, on request, product compliance information; including (but not limited to); EU Reach and UN compliance declarations.
- Employees of our suppliers shall be paid wages and benefits for a standard working week that meet or exceed minimum national requirements.

- No forced, bonded or involuntary prison labour will be used.

Failure to comply with any agreed improvement plan would result in review and possible termination of the contract. Don-Bur companies must have appropriate checks in place to ensure that suppliers meet or exceed these requirements.

6.3 Policy Commitments – Don-Bur's Commitment to Suppliers

Don-Bur commits to the following in relation to purchasing and supply chain activities: Supplier Business Practices.

Don-Bur will not use another party to perform a task that Don-Bur company employees are not permitted to perform.

Don-Bur will ensure that agents or any other representatives acting on the company's behalf know about applicable company policies when working for Don-Bur.

6.3.1 Purchasing Business Practices

Procurement processed will rely on factual, objective information, based on materials that are provided to all relevant suppliers. This process will not discriminate against a potential supplier based on improper considerations, such as its management's gender, race, nationality or age. In addition, Don-Bur will support our customers' diversity agenda by providing information on minorities as requested.

Don-Bur will use a procurement process that is fair and seeks the best value for the cost of purchases.

6.3.2 Business Partners Review

Don-Bur will conduct appropriate reviews of potential business partners to ensure that the level of risk is appropriate for the business. Reviews should consider assessment of information relevant to the anticipated relationship with the potential partner, which may include financial soundness, legal matters, employment practices and ethics and compliance.

6.3.3 Fair & Ethical Dealings

Don-Bur employees will conduct business fairly, and never misrepresent themselves, the company or its products or services. Employees will not try to obtain advantage through dishonest, corrupt or other fraudulent or unlawful activities.

6.3.4 Fair Competition

Don-Bur will ensure fair competition in its supply chain at all times, avoiding fixing prices or rigging purchasing bids.

6.4 Reporting of Breaches and Accountability

Any employee or business partner who becomes aware of any existing or potential breach of this policy is required to notify Don-Bur promptly.

6.5 Enquiries

All enquiries in relation to this policy or its applicability to particular situations should be addressed to the HR department.

7 Data Security & Protection

7.1 Computers and IT – GDPR

7.1.1 Endpoint and network security

All endpoints are part of a secure Microsoft active directory system with password and data access policies in place.

Operating system updates and security patches are centrally managed and deployed daily to all endpoints.

Network access is granted dependent on the user's access level and permissions set and controlled by the IT department.

Physical access to server comms rooms is restricted to selected senior management and is protected via keycode locks.

All company data is backed up and replicated every night to 2 secure site locations.

Gateway security is managed by firewall devices at all sites with the below features:

- IPS & Application Control
- Antivirus \ Anti-Malware
- Web Filtering
- Anti-Spam Filtering
- Secure SSL VPN

File\Data security is handled by industry standard file audit software that monitors and reports on all file access across all network data.

Endpoint security is managed by centrally managed and updated by endpoint protection with the below features:

Antivirus \ Anti-Malware protection against.

- Ransomware
- Mobile malware

- Advanced threats
- File less threats
- PowerShell & script-based attacks
- Web threats

Email is protected on several layers:

- Remote smart host with anti-spam and antivirus\anti malware filtering
- Gateway protection with anti-spam and antivirus\anti malware filtering
- Endpoint protection with antivirus\anti malware filtering

Utilising different systems will ensure maximum protection using multiple definitions.

7.1.2 Software

Employees must use only software that is authorised by Don-Bur Group on Don-Bur Group computers\systems. All software on Don-Bur Group computers must be approved or installed by the Don-Bur Group IT department.

7.1.3 Password Policy

All devices are controlled by Active directory and the following policy is forced:

- Minimum password length of 7 characters and of a “complex” format
- Maximum password age of 90 days

Users are informed to the below conditions regards passwords via a company AUP policy:

- Not allow anyone else to use their user ID and password on any Don-Bur Group IT systems.
- Not leave their user accounts logged in at an unattended and unlocked computer.
- Not use someone else’s user ID and password to access Don-Bur Group IT systems.
- Not leave their password unprotected (for example writing it down).

7.1.4 Remote working

See the relevant section in the company AUP policy:

7.1.5 Mobile Storage Devices

See the relevant section in the company AUP policy:

7.2 Don-Bur Group IT Policy (AUP)

This Acceptable Usage Policy covers the security and use of all Don-Bur Group information and IT equipment. It also includes the use of email, internet, voice and mobile IT equipment.

This policy applies to all Don-Bur Group employees, contractors and agents (hereafter referred to as 'individuals').

This policy applies to all information, in whatever form, relating to Don-Bur Group business activities worldwide, and to all information handled by Don-Bur Group relating to other organisations with whom it deals. It also covers all IT and information communications facilities operated by Don-Bur Group or on its behalf.

7.2.1 Computer Access Control – Individual's Responsibility

Access to the Don-Bur Group IT systems is controlled by the use of User IDs and passwords. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the Don-Bur Group's IT systems.

Individuals must not:

- Allow anyone else to use their user ID and password on any Don-Bur Group IT systems.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's user ID and password to access Don-Bur Group IT systems.
- Leave their password unprotected (for example writing it down).
- Perform any unauthorised changes to Don-Bur Group IT systems or information.
- Attempt to access data that they are not authorised to use or access.
- Exceed the limits of their authorisation or specific business need to interrogate the system or data.
- Connect any non-Don-Bur Group authorised device to the Don-Bur Group network or IT systems.
- Store Don-Bur Group data on any non-authorised Don-Bur Group equipment.
- Give or transfer Don-Bur Group data or software to any person or organisation outside Don-Bur Group without the authority of Don-Bur Group.

7.2.2 Internet and Email Conditions of Use

Use of Don-Bur Group internet and email is intended for business use. Personal use is permitted only during break times where such use does not affect the individual's business performance, is not detrimental to Don-Bur Group in any way, not in breach of any term and condition of employment and does not place the individual or Don-Bur Group in breach of statutory or other legal obligations.

All individuals are accountable for their actions on the internet and email systems.

Individuals must not:

- Use the internet or email for the purposes of harassment or abuse.
- Use profanity, obscenities, or derogatory remarks in communications.
- Access, download, send or receive any data (including images), which Don-Bur Group considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.
- Use the internet or email to make personal gains or conduct a personal business.
- Use the internet or email to gamble.
- Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- Place any information on the Internet that relates to Don-Bur Group, alter any information about it, or express any opinion about Don-Bur Group, unless they are specifically authorised to do this.
- Send unprotected sensitive or confidential information externally.
- Forward Don-Bur Group mail to personal (non-Don-Bur Group) email accounts (for example a personal Hotmail account).
- Make official commitments through the internet or email on behalf of Don-Bur Group unless authorised to do so.
- Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.
- In any way infringe any copyright, database rights, trademarks or other intellectual property.
- Download any software from the internet without prior approval of the IT Department.
- Connect Don-Bur Group devices to the internet using non-standard connections.

7.2.3 Clear Desk and Clear Screen Policy

In order to reduce the risk of unauthorised access or loss of information, Don-Bur Group enforces a clear desk and screen policy as follows:

- Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
- Care must be taken to not leave confidential material on printers, desks or photocopiers.
- All confidential business-related printed matter must be disposed of using confidential waste bins or shredders.

7.2.4 Remote working

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

- The loss of any device must be reported to the Don-Bur IT department immediately, the device can then be deactivated and access to any data ceased.
- Care must be taken when connecting to Public access points “hotspots” that do not require a logon\password as transmitted data will be unencrypted. The access point may be malicious or being manipulated by an attacker.
- Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a password or PIN\fingerprint.
- Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car\vehicle.
- Laptops must be carried as hand luggage when travelling.
- Information should be protected against loss or compromise when working remotely (for example at home or in public places).

7.2.5 Mobile Storage Devices

Mobile devices such as memory sticks, CDs, DVDs and removable hard drives are used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. Information should be protected against loss or compromise and only used for non-confidential data.

7.2.6 Software

Employees must use only software that is authorised by Don-Bur Group on Don-Bur Group computers\systems. Authorised software must be used in accordance with the software supplier's licensing agreements. All software on Don-Bur Group computers must be approved or installed by the Don-Bur Group IT department.

Individuals must not:

Store personal files (such as music, video, photographs or games) on Don-Bur Group IT equipment.

7.2.7 Viruses

The IT department has implemented centralised, automated virus detection and virus software updates within the Don-Bur Group. All PCs have antivirus software installed to detect and remove any virus automatically.

Individuals must not:

- Remove or disable anti-virus software.

- Attempt to remove virus-infected files or clean up an infection, other than by the use of approved Don-Bur Group anti-virus software and procedures.

7.2.8 Telephony Voice and mobile data Equipment Conditions of Use

Use of Don-Bur Group equipment is intended for business use. Individuals must not use Don-Bur Group voice\data facilities for sending or receiving private communications on personal matters or other personal use except in authorised circumstances. All non-urgent personal communications should be made at an individual's own expense, in their own time, and using alternative means of communications.

Individuals must not:

- Use Don-Bur Group voice\data equipment for conducting private business.
- Make hoax or threatening calls to internal or external destinations.
- Accept reverse charge calls from domestic or International operators, unless it is for business use and authorised.

7.2.9 Actions upon Termination of Contract

All Don-Bur Group equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to Don-Bur Group at termination of contract.

All Don-Bur Group data or intellectual property developed or gained during the period of employment remains the property of Don-Bur Group and must not be retained beyond termination or reused for any other purpose.

7.2.10 Monitoring and Filtering

All data that is created and stored on Don-Bur Group computers is the property of Don-Bur Group and there is no official provision for individual data privacy, however wherever possible Don-Bur Group will avoid opening personal emails.

IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. Don-Bur Group has the right (under certain conditions) to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse.

Any monitoring will be carried out in accordance with current legislation.

It is your responsibility to report suspected breaches of security policy without delay to the IT department.

All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with Don-Bur Group disciplinary procedures.

7.3 Cyber Essentials Scheme

Don-Bur is certified to comply with the Cyber Essentials Scheme requirements under certificate #2181593

7.4 Data Protection Policy

This Precedent is an internal-facing data protection policy for use in relation to employees or other workers and contractors. It takes into account the more extensive requirements under General Data Protection Regulation (GDPR), which came into effect on 25 May 2018, those proposed in the Data Protection Bill (DPB) and the Information Commissioner's Office (ICO) guide to the GDPR. It identifies, at a high level:

- how the employer complies with its obligations under the GDPR, in particular the data protection principles which the employer, as a data controller, is required to follow
- how staff are expected to handle personal data and sensitive personal data
- the role of the data protection officer, if there is one
- the need for staff to seek further guidance from the data protection officer or other role holder or department if they have any queries or if they are dealing with complex situations, the scope of which is beyond the remit of this policy, and
- the consequences of breach

Employers are required to implement appropriate technical and organisational measures that ensure and demonstrate that they process personal information in accordance with GDPR. The ICO guidance indicates that this may include internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies.

This Precedent is not a data protection policy of the type that a company would wish to make routinely available to third parties, as it focuses on data protection issues relevant to the processing of staff information, rather than customer/client information.

In most cases, the employer will already have a data protection policy and this precedent will need to be introduced as a replacement.

We recommend that the draft policy should be discussed with employee representatives or a representative sample of employees before it is introduced.

We also recommend that the policy should be discussed with new employees as part of their induction process and with existing employees as part of a data protection training programme. The policy should also be made available in the staff handbook and/or on the employer's staff intranet. However, the employer should choose whatever method(s) it considers most effective, in light of the organisation's 'house style' and HR approach.

This Precedent assumes that the employer:

- does not employ children
- does not carry out profiling or any other form of automated decision-making

- does not record events, movements or driving behaviour in any vehicle the employees drive
- does not monitor home or remote working, or employee devices used for work under a Bring Your Own Device (BYOD) policy, or use Mobile Device Management (MDM) services

If you consider that you do have a lawful basis to carry out profiling and/or automated decision-making, ICO guidance recommends that this should be documented in its data protection policy.

7.4.1 Data Protection Clause

We will collect and process personal data and sensitive personal data (also known as 'special categories of personal data') [and criminal records data] relating to you in accordance with our data protection policy and our data protection privacy notice contained in the Employee Handbook.

You confirm that you have read and understood the data protection policy of the Company. You will comply with your obligations under our data protection policy and other relevant policies

The Company is entitled to make changes to its data protection policy but will notify employees in writing of any such changes.

We may monitor staff in accordance with our policies relating to email, internet and communications systems and monitoring at work, contained in our Employee Handbook.

Failure to comply with the data protection policy or any of the policies listed above in this clause 20 may be dealt with under our disciplinary procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

7.4.2 Data Protection Privacy Notice to Employees

A Data Protection Privacy Notice is issued to all Employees which details, among other items, GDPR.

7.5 Physical Security for HR Documentation Storage

Our physical records are secured with the highest security padlock available on the market.

7.6 Records Retention

Don-Bur operates a system of secure physical document storage. We keep records in line with statutory guidance, and a full register of all documents stored by box location is maintained in the accounts department.

7.7 Disposal of Confidential Waste

Don-Bur uses traceable 3rd party services to dispose of confidential waste.

7.8 ICO Registration

Don-Bur is registered with the ICO, reference# Z9305034, Tier 3.

A Bushnell
Finance Director
19.3.21