## Statement

Clearwater DC 2001 Ltd needs to retain and process certain data in order to enable the efficient running of the business. This includes certain personal data on our employees, customers, suppliers and other associates of the business. We are committed to the principles of Data Protection legislation and this policy sets out our obligations and the requirements we have of our employees. We also have an Employee Privacy Policy which sets out our commitment to you in relation to your personal data.

The Company has a responsibility for monitoring compliance with data protection principles as well as the effectiveness of this policy.

## Key Principles

Employees in the course of their duties may have access to information which is private or confidential to the Company, employees, and customers and it is the responsibility of employees to preserve the confidentiality and integrity of information used during the course of their work and to protect the interests of the business.

Under Data Protection legislation there are certain responsibilities in relation to personal data held on computers and also certain manual records where they form part of a structured filing system. Under the regulations, all personal data is subject to the 'data protection principles'. All employees must be aware of and act in accordance with the principles. These are that personal data:

1. must be processed fairly, lawfully and in a transparent manner
2. must be obtained for lawful purposes
3. must be adequate, relevant and not excessive
4. must be accurate and where necessary kept up to date
5. must not be kept longer than necessary
6. must be safeguarded against unauthorised or unlawful processing and against accidental loss, damage or destruction

## 22 .2 Employee Obligations

All employees are required to take practical steps to comply with the principles, including if you have a desk and computer, keeping a clear desk outside working hours, ensuring personal data is never left visible or unattended on a desk, photocopier or computer screen.

You should never disclose personal information about another member of staff, a customer or supplier.

If during the course of your work you have access to information which is private or confidential to the Company, fellow or former employees, customers or suppliers, you have a responsibility for the preservation of the confidentiality and integrity of the information used during the course of your work.

If, as part of your role, you collect personal information about employees or other people such as customer, suppliers or colleagues, you must comply with this policy including the data protection principles. You must also comply with the following guidelines at all times:

- Do not disclose confidential personal information to anyone except the data subject, unless the data subject has given their explicit prior written consent to this
- Ensure you verify the identity of the individual and the legitimacy of the request before releasing any personal information
- If you receive a request for personal information about another employee, you should forward this to the Managing Director, who is responsible for dealing with such requests
- Ensure any personal data you hold is kept securely and is not seen by unauthorised persons
- Ensure that, when working on personal information as part of your job duties when away from your workplace, you continue to observe the terms of this policy, in particular in relation to data security
- Ensure that hard copy personal information is disposed of securely
- Take practical steps to support the adherence to the principles, for example keeping passwords separately from laptops and phones, using a strong password and not sharing your password with others
- Remember that compliance is your personal responsibility

*Please note that failure to follow the above obligations or comply with the Data Protection policy may be considered a disciplinary matter.*

## 22.3 Company Obligations

The Company holds personal data about you. We need to process your personal data to carry out our legal duties under the employment contract including payroll and benefits administration and to ensure we can carry out our general business and HR activities .

The publishing of information such as an annual report, marketing material, etc. which contains employee information is not prohibited, but the following guidelines should be followed. Information about employees should only be published where:

- there is a legal obligation to do so, or
- the information is clearly not intrusive, or
- the individual has consented to the disclosure, or
- the information is in such a form that it does not identify individuals.

Where the employee gives their consent they should be made aware of the extent of information that will be published, how it will be published and the implications of this.

Under Data Protection legislation the 'reason' for sickness absence is classified as 'special categories of data'. We need to process special categories of data to carry out your contract and meet our legal obligations. We will limit access to this information and keep it secure. As a consequence, the reason for illness will only be disclosed to the individual's line manager. There should be no discussion or disclosure of the reason for sickness except between the individual, line manager and Director.

Anyone whose personal data is being processed by the Company has certain rights in relation to their personal data. In practice, what this means is that individuals have the right, on written request and within a month, to:

- be told what personal data is being processed, why it is being processed, where it came from and to whom it may be disclosed
- access that data in an intelligible form
- ask to rectify the data if inaccurate
- ask for the data to be erased
- restrict processing
- data portability (in certain circumstances); and
- not to be subject to automated decision-making, for example in recruitment selection

## 22.4 Further information or queries

For further information, or in the case of any queries over this policy or a particular matter of data protection, please consult the Managing Director.

Signed 

Murray Pitcairn
Managing Director

Date: 10/01/2022
Review Date: 10/01/2023