

## DATA PROTECTION POLICY

### Introduction

1. Atlas Cleaning Limited retains certain information about its employees, clients, suppliers and contractors to allow it to process information so that the Company can comply with its legal obligations to pay wages and suppliers as well as the facility to invoice clients for the services provided. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

2. To achieve or requirements Atlas Cleaning Limited must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (the Act).

3. The Data Principles are:

- Personal data shall be processed fairly and lawfully;
- Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose;
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;
- Personal data shall be accurate and, where necessary, kept up to date;
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes;
- Personal data shall be processed in accordance with the rights of data subjects under this Act;
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data;
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

4. Atlas Cleaning Limited and all staff or others who process or use personal information must ensure that they follow these principles at all times.





5. In order to ensure that this happens, the Company has developed this Data Protection Policy and the accompanying Data Protection Code of Practice.

### **Status of this Policy**

6. This policy does not form part of the formal contract of employment for staff but it is a condition of employment that employees will abide by the rules and policies made by the Company from time to time and any failures to follow the policy can therefore result in disciplinary proceedings.

### **The Data Controller**

7. The Company as a body corporate is the Data Controller under the Act and the Board is therefore ultimately responsible for implementation. However, the Designated Data Controllers will deal with day-to-day matters.

8. The Designated Data Controller is the Human Resources Director.

9. Any employee who considers that the policy has not been followed in respect of personal data about himself or herself should raise the matter with the Designated Data Controller.

### **Responsibilities of Staff**

10. All staff are responsible for:

- Checking that any information that they provide to the Company in connection with their employment is accurate and up to date;
- Informing the Company of any changes to information that they have provided, e.g. changes of address.

### **Data Security**

11. All employees are responsible for ensuring that:

- Any personal data that they hold is kept securely;
- Personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party;

12. Employees must note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

13. Personal information should:

- Be kept in a locked room, locked filing cabinet, drawer, or safe; or



- If it is computerised, be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up; and
- If a copy is kept on a diskette or other removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

### **Rights to Access Information**

14. All employees are entitled to:

- Know what information the Company holds and processes about them and why;
- Know how to gain access to it;
- Know how to keep it up to date;
- Know what the Company is doing to comply with its obligations under the Act.

15. The Company will, upon request, provide all employees and other relevant users with a statement regarding the personal data held about them. This will state all the types of data the Company holds and processes about them, and the reasons for which they are processed.

16. All employees and other users have a right under the Act to access certain personal data being kept about them either on computer or in certain files. Any person who wishes to exercise this right should complete the Subject Access Request Form and submit it to the Designated Data Controller.

17. The Company will make a charge of £10 on each occasion that access is requested.

18. The Company aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days, as required by the Act.

Examination Marks

### **Subject Consent**

19. In many cases, the Company can only process personal data with the consent of the individual. In some cases, if the data is sensitive, as defined in the Act, express consent must be obtained. Agreement to the Company processing some specified classes of personal data is a condition of employment for staff. This includes information about previous criminal convictions.

20. Some jobs will bring the employee into contact with children and vulnerable adults. The Company has a duty of care to all employees and its Clients and therefore may request information under the Disclosure and Barring Service.



21. The Company may also ask for information about particular health needs, such as any medical condition such as asthma or a physical impairment. The Company will only use this information in the protection of the health and safety of the individual, but will need consent to process this data in the event of a medical emergency, for example.

22. Therefore, the application forms that all prospective employees are required to complete will include a section requiring consent to process the applicant's personal data. A refusal to sign such a form will prevent the application from being processed.

### **Processing Sensitive Information**

23. Sometimes it is necessary to process information about a person's health, criminal convictions and race. Because this information is considered sensitive under the Act, employees will be asked to give their express consent for the Company to process this data. An offer of employment may be withdrawn if an individual refuses to consent to this without good reason.

### **Publication of Company Information**

24. The names of Directors or Senior Management of the Company or any other relevant personal data may be published on the Web site or when any statute or law requires such data to be made public.

25. Certain items of information relating to the Company's management may be made available via searchable directories or on the Web site, in order to meet the legitimate needs of suppliers or potential clients.

### **Retention of Data**

26. The Company has a duty to retain some employee personal data for a period of time following their departure from the Company, mainly for legal reasons, but also for other purposes such as being able to provide references, or relating to pensions and taxation. Different categories of data will be retained for different periods of time.

### **Conclusion**

27. Compliance with the Act is the responsibility of all employees of the Company. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or even to a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the Designated Data Controller.



---

Brian Sweeting, Human Resources Manager

Atlas Contractors Limited

Dated: **January 2017**

Review Date: **January 2018**