**1SC GUARDING LIMITED**

| TITLE: Data Protection (GDPR) Policy | REF NO: QM 22 | PAGE: 1 OF 9 |
|---|---|---|

| ISSUE: 1 | | | |
|---|---|---|---|

# Contents

Contents ..... 2
1. Introduction ..... 3
Data Protection Act and GDPR principles ..... 3
2. What information is covered ..... 4
3. Policy statement ..... 4
4. Principles ..... 4
5. Scope of this policy ..... 5
6. Policy ..... 5
7. Data protection responsibilities ..... 5
Line managers' responsibilities ..... 6
General Responsibilities ..... 6
8. Monitoring ..... 7
9. Validity of this policy ..... 7
Appendix A - Data Protection Act 2018 - Data ..... 7
Appendix B – Summary of relevant legislation and guidance ..... 7
Human Rights Act 2018 ..... 8
Freedom of Information Act 2000 ..... 8
Crime and Disorder Act 2018 ..... 8
The Computer Misuse Act 1990 ..... 8

# 1. Introduction

The Data Protection Act 2018 controls how your personal information is used by organisations, businesses, or the government. The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

## Background

1.1 1SC Guarding Ltd (1SC) needs to collect person-identifiable information about individuals to carry out its functions and fulfil its objectives. Personal data is defined as 'information which relates to a living individual and from which they can be identified, either directly or indirectly'.

1.2 Personal data at 1SC can include employees (present, past, and prospective), contractors and third parties, private and confidential information as well as sensitive information, whether in paper, electronic, or other form.

1.3 Irrespective of how information is collected, recorded and processed person identifiable information must be dealt with properly to ensure compliance with the Data Protection Act (DPA) 2018 and the forthcoming General Data Protection Regulations (GDPR).

1.4 The DPA requires 1SC to comply with the eight Data Protection Principles (see Appendix A below) and to notify the Information Commissioner about the data that we hold and why we hold it. This is a formal notification and is renewed annually.

1.5 The DPA gives rights to data subjects (people that we hold information about) to access their personal information, to have it corrected if wrong, in certain permitted circumstances to ask us to stop using it, and to seek damages where we are using it improperly.

1.6 The lawful and correct treatment of person-identifiable information by 1SC is paramount to the success of the organisation and to maintaining the confidence of its service users and employees. This policy will help 1SC ensure that all person-identifiable information is handled and processed lawfully and correctly.

### Data Protection Act and GDPR principles

1.7 1SC has a legal obligation to comply with all relevant legislation in respect of data protection and information / IT security. The organisation also must comply with guidance issued by advisory groups and professional bodies.

1.8 All legislation relevant to an individual's right to the confidentiality of their information and how that can be achieved and maintained are paramount to 1SC. Significant penalties may be imposed upon 1SC or its employees for non-compliance.

1.9 this policy aims to outline how 1SC meets its legal obligations in safeguarding confidentiality and adheres to information security standards. The obligations within this policy are principally based upon the requirements of the Data Protection Act

2018 and the forthcoming GDPR, as the key legislative and regulatory provisions governing the security of person-identifiable information.

1.10 Other relevant legislation and guidance referenced and to be read in conjunction with this policy are outlined together with a summary in Appendix B.

## 2. What information is covered

2.1 Personal data within the respective legislative and regulatory provisions covers 'any data that can be used to identify a living individual either directly or indirectly'. Individuals can be identified by various means, including but not limited to, their address, telephone number, or e-mail address. Anonymized or aggregated data is not regulated by the provisions, provided that the anonymization or aggregation of the data is irreversible.

## 3. Policy statement

3.1 This document defines the data protection policy for 1SC. It applies to all person-identifiable information obtained and processed by the organisation and its employees. It sets out:

- the organisation's policy for the protection of all person-identifiable
- information that is processed
- establishes the responsibilities (and best practices) for data protection
- references the key principles of the Data Protection Act 2018 and GDPR.

## 4. Principles

4.1 The objective of this policy is to ensure the protection of 1SC's information by relevant legislation, namely:

A. To ensure notification.

Annually notify the Information Commissioner about 1SC's use of person-identifiable information.

B. To ensure professionalism.

All information is obtained, held, and processed professionally by the eight principles of the Data Protection Act 2018 and the provisions of the GDPR.

C. To preserve security.

All information is obtained, held, disclosed, and disposed of securely.

D. To ensure awareness.

Provision of appropriate training and promote awareness to inform all employees of their responsibilities.

E. Data Subject access.

Prompt and informed responses to subject access requests.

4.2 The policy will be reviewed periodically by 1SC directors. Where review and update are necessary due to legislative changes this will be done immediately.

4.3 By 1SC's equality and diversity policy statement, this procedure will not discriminate, either directly or indirectly, on the grounds of gender, race, colour, ethnic or national origin, sexual orientation, marital status, religion or belief, age, union membership, disability, offending background or any other personal characteristic.

## 5. Scope of this policy

5.1 This policy will ensure that person-identifiable information is processed, handled, transferred, disclosed, and disposed of lawfully. Person-identifiable information should be handled in the most secure manner by authorised staff only, on a need-to-know basis.

5.2 The procedures cover all person identifiable information whether internal or external, electronic or paper which may relate to employees, contractors, and third parties about whom we hold information.

## 6. Policy

6.1 1SC obtains and processes person-identifiable information for a variety of different purposes, including but not limited to:

A. staff records and administrative records

B. Vetting of third-party companies to the latest British Standard 7858

C. Complaints and requests for information.

D. Client records regarding sites, staff, and other sensitive information

6.2 Such information may be kept in either computer or manual records. In processing such personal data 1SC will comply with the data protection principles within the Data Protection Act 2018.

## 7. Data protection responsibilities

Overall Responsibilities

7.1 1SC Directors, collectively known as the 'data controller' permit 1SC's staff to use computers and relevant filing systems (manual records) in connection with their duties. 1SC directors have legal responsibility for the notification process and compliance with the Data Protection Act 2018.

7.2 1SC directors whilst retaining their legal responsibilities have delegated data protection compliance to the Data Protection Officer.

7.3 The Data Protection Officer's responsibilities have been allocated.

7.4 The Data Protection Officer's responsibilities include:

A. Ensuring that the policy is produced and kept up to date

B. Ensuring that the appropriate practices and procedures are adopted and followed by 1SC.

C. Provide advice and support to the Directors on data protection issues within the organisation.

D. Work collaboratively with the 1SC Quality system to help set the standard of data protection training for staff.

E. Ensure data protection notification with the Information Commissioner's Office is reviewed, maintained, and renewed annually for all use of person-identifiable information.

F. Ensure compliance with individual rights, including subject access requests.

G. Act as a central point of contact on data protection issues within the organisation.

H. Implement an effective framework for the management of data protection.

### Line managers' responsibilities

7.5 All line managers within 1SC are directly responsible for:

A. Ensuring their staff are made aware of this policy and any notices.

B. Ensuring their staff are aware of their data protection responsibilities.

C. Ensuring their staff receive suitable data protection training.

### General Responsibilities

7.6 All 1SC employees, including temporary and contract staff are subject to compliance with this policy. Under the GDPR individuals can be held personally liable for data protection breaches.

7.7 All 1SC employees have a responsibility to inform their supervisors and the Data Protection Officer of any new use of personal data, as soon as reasonably practicable after it has been identified.

7.8 All 1SC employees will, on receipt of a request from an individual for information held, known as a subject access request or concerns about the processing of personal information, immediately notify the Data Protection Officer.

7.9 Employees must follow the subject access request procedure (see Appendix C below).

## 8. Monitoring

8.1 Compliance with this policy will be monitored by the MD, together with internal audit reviews where necessary.

8.2 The Information Governance and Risk Management Lead is responsible for the monitoring, revision, and updating of this policy document on an annual basis or sooner, should the need arise.

## 9. Validity of this policy

9.1 This policy will be reviewed at least annually under the authority of 1SC Directors. Associated data protection standards will be subject to an ongoing development and review program.

### Appendix A - Data Protection Act 2018 - Data protection principles

1. Personal data shall be processed fairly and lawfully.

2. Personal data shall be obtained for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant, and not excessive for the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and accidental loss or destruction of, or damage to, personal data.

8. 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 regarding the processing of personal data.

### Appendix B – Summary of relevant legislation and guidance

#### General Data Protection Regulations (GDPR)

A legal basis must be identified and documented before personal data can be processed. 'Directors' and 'Data protection officers' will be required to document decisions and maintain records of processing activities.

### Human Rights Act 2018

Groups to respect and protect an individual's human rights. This will include an individual's right to privacy (under Article 8) and a service user's right to expect confidentiality of their information always.

Article 8 of the Act provides that "everyone has the right to respect for their private and family life, their home and their correspondence". However, this article also states, "There shall be no interference by a public authority with the exercise of this right except as is by the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention or disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others". Each organisation must act in a way consistent with these requirements. It must take an individual's rights into account when sharing personal information about them.

### Freedom of Information Act 2000

This Act gives individuals the right of access to information held by public authorities. Regulation of Investigatory Powers Act 2000 This Act combines rules relating to access to protected electronic information as well as revising the "Interception of Communications Act 1985". The Act aimed to modernise the legal regulation of interception of communications, in the light of the Human Rights laws and rapidly changing technology.

### Crime and Disorder Act 2018

This Act introduces measures to reduce crime and disorder, including the introduction of local crime partnerships around local authority boundaries to formulate and implement strategies for reducing crime and disorder in that local area.

The Act allows disclosure of person-identifiable information to the Police, Local Authorities, Probation Service, or the Health Service but only if the purposes are defined within the Crime and Disorder Act. The Act does not impose a legal requirement to disclose personally identifiable information and responsibility for disclosure rests with the organisation holding the information.

### The Computer Misuse Act 1990

This Act makes it a criminal offense to access any part of a computer system, programs, and/or data that a user is not entitled to access. 1SC issues each employee with an individual user id and password, which will only be known to the individual and must not be divulged to other staff. This is to protect the employee from the likelihood of their inadvertently contravening this Act. 1SC will adhere to the requirements of the Computer Misuse Act 1990 by ensuring that its staff are aware of their responsibilities regarding the misuse of computers for fraudulent activities or other personal gain. Any member of staff found to have contravened this Act will be considered to have committed a disciplinary offense and will be dealt with accordingly.

**Authorised by:**

**David Jones**

**Managing Director.**