



EMPLOYEE HANDBOOK

Employee Orientation Manual



spsgroupservices.com



Contents

	P A G E
01. Using This Handbook	04
02. SPS Security	05
03. ICS Cleaning	09
04. SPS Group General Rules	13
05. Employee Mental Health and Wellbeing	15
06. Training	21
07. Drug and Alcohol Policy	22
08. Equity and Diversity Policy	23
09. Anti-Harrassment and Bullying Policy	25
10. Anti-Corruption and Bribery Policy	28
11. Whistleblowing Policy	30
12. IT and Communications Systems Policy	32
13. Social Media Policy	35
14. Data Privacy Notice For Employees, Workers and Contractors	37
15. Data Protection Policy	48
16. Disciplinary and Capability Policy	58
17. Grievance Policy	60
18. Anti-Slavery and Human-Trafficking Policy	62
19. SPS Group Sickness Absence Management Procedure	64
20. SPS Group Services Customer Care Policy	80
21. SPS Group Services Workplace Violence Policy	84

Comprehensive Services, Family Values

Introduction

Welcome to the SPS Group of companies, which currently consists of SPS Security Limited, Independent Cleaning Services Limited, SPS Technical Services, and SPS Training Services.

SPS Group Services started as a family-owned business in 1992 and continues to be family-owned to this day. With centuries of combined experience, we provide tailored solutions in security, cleaning, maintenance, and training for clients across the North of England.

Our 24-hour control room and headquarters are based in Hull, and we have strategically located regional branch offices to enhance our operational coverage and capabilities.

Since our establishment, we have established a strong financial base and have grown into a facilities management provider that is “large enough to manage,” yet “small enough to care,” offering complete end-to-end solutions.

Group Philosophy

SPS group believes in commitment to achieving customer satisfaction every time.

This can only be realised by maintaining the highest standards and through the commitment of a well-trained and motivated workforce and by the application of best practices.



01 USING THE STAFF HANDBOOK

This Staff Handbook sets out the main policies and procedures that you will need to be aware of while working for us. You should familiarise yourself with it and comply with it at all times. Any questions you may have with regard to its contents or what you have to do to comply with it should be referred to your line manager or the Health and Safety and Compliance Manager in the first instance.

- 1.1 The individual policies and procedures set out in this Staff Handbook indicate whether they apply to all staff or certain categories of staff.
- 1.2 The SPS Rules and Group Rules in this Staff Handbook do form part of your contract of employment with us.
- 1.3 The Group Policies section in this Staff Handbook does not form part of the terms of your contract with us and may be amended or updated at any time.
- 1.4 Everyone should ensure that they take the time to read and understand the content of this Staff Handbook and act in accordance with its aims and objectives. All staff must ensure that they are familiar with and comply with and support its policies and procedures.

SECTION 02

SPS Security

This section of the handbook applies to employees and workers engaged by SPS Security Limited (the Company/we/us) only. They must be read in conjunction with Assignment Instructions and other site instructions, which must be followed at all times. Where these are different to general Company rules, the Assignment Instructions and other site instructions should take precedence.

SIA/ BSIA RULES AND CODES OF CONDUCT

SPS Security Limited is a member of the British Security Industry Association (BSIA) and is regulated by the Security Industry Authority (SIA).

It is a condition of employment with SPS Security Limited that you comply at all times with the rules, regulations, codes of practice and other requirements and standards set by the SIA and BSIA. These can be found at:

2.1 SUPERVISOR TASKS

Supervisors are appointed for their knowledge and experience. They are required to set the highest standards of dress, conduct and performance and are to lead by example. The interests of both the Company and the client must be the supervisor’s primary concern. Supervisors will report to their line manager.

Specific tasks:

- Monitoring performance and undertaking appraisals of the company’s staff.
- On the job training.
- Monitoring of logs, reports, and patrol records on assignments.
- Monitoring officers’ work records.
- Roster relief and manning within the assignments.
- Liaison between officers and management on personnel matters.
- Liaison with customer representatives on a day to day basis.
- Periodic checks on the patrol driver’s performance.
- Liaison with the on call management as necessary.

2.2 SECURITY OFFICER TASKS

This includes all SPS Security Limited staff. Specific duties are detailed in Assignment Instructions and other site instructions. Where doubt or ambiguity exists, officers should seek advice from the Control Room Supervisor or On Call Manager.

SECTION 02

SPS Security

On all smaller assignments operational staff should report to the Control Room or Mobile Supervisor. On large multi-manned assignments, officers’ reports to their on-site Supervisor.

Specific Tasks

Read and understand the Assignment Instructions and sign the confirmation sheet located within the instructions.

- Check all keys, equipment, and stores on commencement on duty.
- Particular attention must be given to checking the communications and patrol recording equipment to ensure it has not been damaged prior to taking over duty. In the even that it has been damaged it must be recorded in the site diary and reported to Control.
- Familiarise yourself with any special site instructions or client requests prior to signing the site diary.
- Patrols conducted during the hours of darkness must be carried out using a torch.

Dress and Deportment

- Only wear the authorised form of company uniform.
- Maintain a high standard of appearance and bearing.
- Carry out duties in a firm but courteous manner.
- For safety reasons we may need to prohibit the wearing of certain items of jewellery. Please refer to the Assignment/ site instructions.
- You must address customers and consumers in a courteous manner at all times and should not become over familiar with such.
- Body markings should be covered whilst on duty at the discretion of management and/or the customer.

2.3 VEHICLES

When you use a Company vehicle:

- You are to ensure that you in possession of a valid driving licence.
- You are responsible for the cleanliness and road-worthiness of the vehicle in your charge.
- Traffic accidents or vehicle defects must be reported immediately. Failure to notify the Company of any damage to a vehicle whilst in your charge will be treated as misconduct.
- A vehicle check sheet is to be completed for each duty period.
- Vehicles must be fuelled at the end of every shift. Premium fuel must not be drawn.
- You must adhere to the Highway Code.

SECTION 02

SPS Security

- Smoking in Company vehicles is strictly prohibited and is against the law.
- You agree that any private motor vehicles, equipment, or personal belongings which you have taken on any assignment is your sole responsibility and that the Company has no liability in the event of theft or damage to such items. You are to abide by the site traffic regulations and parking arrangements at all times.

2.4 PATROL OFFICERS AND SITES WITH A VEHICLE

In the event that your employment with the Company is that of a patrol driver or involves the use of a vehicle to carry out your duties then the following must be adhered to: -

- No alcoholic beverages, drugs or other controlled or banned substances are to be consumed 24 hours prior to the start of any driver’s duty.
- You must adhere to the rules of the Highway Code at all times and in particular must obey any speed restrictions. Under no circumstances must you exceed the legal speed limit including when responding to alarms.
- Where patrol monitoring equipment is fitted on any patrol site you must strike each point to record each visit using the equipment provided. A perimeter check is to be made on every occasion whilst on patrol and checks to be made of all buildings, doors, windows, and parked vehicles to ensure they are secure.
- A manual record of all visits must also be maintained.
- You are not permitted to give lifts to non-employees of the Company.
- You are not permitted to use a company vehicle for your own purposes without authority to do so. Any personal use may incur a deduction from you pay and/or disciplinary action.
- You are to maintain regular contact with the Control Room during your duty.
- In the event that you are convicted or cautioned in relation to any driving offence, even when this applies to a civilian vehicle, you must inform the Company immediately.
- The Company reserves the right to remove you from Mobile Patrol duties when your performance fails to meet with the required company standards and those of our customers.
- The patrol drivers report to the Control Room Supervisors who will decide which driver attends which alarms of emergency response incident.
- The patrol vehicle must be left in a clean and tidy condition at the end of every duty. Any damage must be reported and recorded on the daily patrol sheet.
- It should be noted that all Company vehicles are fitted with a “tracker” which is checked on a regular basis. This records the vehicles actions, locations, and speed. If during the tracker checks, there are any significant issues identified you will be invited in for an investigatory interview.

SECTION 02

SPS Security

2.5 KEYS/FOBS/PASSES

You are responsible for any customer keys which you must sign out from the Control Room at the start of every duty. In the event that any fob/swipe card/pass or key is lost then it may be your responsibility to make good the loss.

2.6 ASSIGNMENT INSTRUCTIONS

You agree to read, sign, and carry out the Assignment Instructions on whichever contract you are assigned. Failure to comply with the content of these instructions or customer operating procedures is a disciplinary matter. These instructions are not to be copied without permission from senior management at the Company.

2.7 SITE DIARY

You are required to maintain a record of events, incidents, accidents, Health & Safety matters, or any unusual occurrences, which occur during your duty period, in the site diary. You must report any matter deemed serious or reportable to the Control Room and the customer as required. The site diary must never be completed in advance and all entries must be accurate and factual. When reporting this to control, it is your responsibility to obtain an SRL log number.

2.8 ASSIGNMENT ACCESS

You’re not to permit any unauthorised access to any assignment for which you are charged with securing. This includes family members, neighbours and/or friends. It also includes other SPS security officers who are not on duty on your contract and have no requirement/need to be on that contract. You are to challenge all persons trying to enter site and to ask for identity, even if those persons are known to you.

2.9 GUARD BASE

You must ensure that the guard base and the surrounding areas are kept clean and tidy at all times. This includes all facilities which you have used during the course of your duty.

SECTION 03

ICS Cleaning

This section of the handbook applies to employees and workers engaged by Independent Cleaning Services Ltd (the Company/we/us) only. They must be read in conjunction with the site operations file. And other site instructions, which must be followed at all times. Where these are different to general Company rules, the site operations file and other site instructions should take precedence.

3.1 SUPERVISOR TASKS

Supervisors are appointed for their knowledge and experience. They are required to set the highest standards of dress, conduct and performance and are to lead by example. The interests of both the Company and the client must be the supervisor’s primary concern. Supervisors will report to their line manager.

Specific Tasks

- To provide an effective cleaning service.
- To ensure that works undertaken by the cleaning team are carried out in accordance with the schedules and to the quality required by the service specification and site set KPI’s.

Functions & Duties

3.1.2 To supervise the activities and be responsible for the effective working and discipline of the contracted cleaning workforce, including compliance with statutory Health and Safety regulations (Health and Safety at Work Act 1974 and associated regulations) and sites Health and Safety Policies/Procedures.

3.1.3 To supervise the cleaning workforce with an emphasis on good industrial relations to provide an effective quality service to the site.

3.1.4 Undertake staff site inductions and training needs questionnaire to ensure all ICS policies and procedures are adhered to.

3.1.5 Allocation of staff and work ensuring all work is covered at the correct times.

3.1.6 Monitoring of staff and work performance ensuring all work is completed to contract specifications.

3.1.7 To ensure that equipment and materials are utilised in a safe and proper manner through the provision of the necessary guidance and training and that all equipment is maintained in a safe working order and reported if not fit for usage.

SECTION 03

ICS Cleaning

- 3.1.8 To ensure that material stocks are maintained at all times.
- 3.1.9 Carry out regular quality audits on a daily basis to ensure that the cleaning meets the agreed standard.
- 3.1.10 Ensure all staff clock on using the automated Time and attendance system and give training on use where appropriate.
- 3.1.11 Controlling issue and usage of materials on site.
- 3.1.12 Attend training sessions as required.
- 3.1.13 Give training session to staff as directed.
- 3.1.14 Ensuring staff work in a sensible and safe manner, observing health and safety regulations and instructions.
- 3.1.15 Uniforms - Ensure that all staff are wearing uniform and that such uniform is freshly laundered and in good condition.
- 3.1.16 Reporting any accidents, near misses, unsafe machinery, and equipment, building fabric or any other potential hazards to the relevant person on site or relevant logs.
- 3.1.17 Any other duties as directed.

NB: This job description is intended for use as a guide only and may be altered at any time by the Account Manager, to suit the needs of the service.

3.2 CLEANING OPERATIVE TASKS

- This includes all Independent Cleaning Services Limited staff.
- Specific duties are detailed in Site Schedules and cleaning Specs and other site instructions.
- Where doubt or ambiguity exists, staff should seek advice from the Supervisor or line Manager.

SECTION 03

ICS Cleaning

Specific Tasks

- 3.2.1 Correct collection and disposal of waste.
- 3.2.2 Basic cleaning duties and required by the contract specification and schedules and by the methods laid down in that contract e.g. damp dusting, damp mopping. Taking care to observe health and safety regulations.
- 3.2.3 Periodic and weekly duties as required by the contract specification and schedules and by the methods laid down in the contract e.g. carpet shampooing/hard floor maintenance.
- 3.2.4 Attend training sessions as required.
- 3.2.5 Correct cleaning standards were directed by the Site Supervisor or Operations Manager.
- 3.2.6 Report any accidents or near misses, unsafe machinery, equipment, building fabric any other potential hazards immediately to your Site Supervisor or Client Representative.
- 3.2.7 Keep machinery and equipment clean, safe, and stored correctly.
- 3.2.8 Any other duties as directed by the Site Supervisor or Operations Manager.
- 3.2.9 This job description is intended for use as a guide only and may be altered at any time by the Site Supervisor or Account Manager, to suit the needs of the service.

3.3 Dress and Deportment

- Only wear the authorised form of company uniform.
- Maintain a high standard of appearance and bearing.
- Carry out duties in a firm but courteous manner.
- For safety reasons we may need to prohibit the wearing of certain items of jewellery. Please refer to site instructions.
- You must address customers and consumers in a courteous manner at all times and should not become over familiar with such.
- Body markings should be covered whilst on duty at the discretion of management and/or the customer.

SECTION 03

ICS Cleaning

3.4 VEHICLES

When you use a Company vehicle:

- You are to ensure that you in possession of a valid driving licence.
- You are responsible for the cleanliness and roadworthiness of the vehicle in your charge.
- Traffic accidents or vehicle defects must be reported immediately. Failure to notify the Company of any damage to a vehicle whilst in your charge will be treated as misconduct.
- A vehicle check sheet is to be completed for each duty period.
- Vehicles must be fuelled at the end of every shift. Premium fuel must not be drawn.
- You must adhere to the Highway Code.
- Smoking in Company vehicles is strictly prohibited and is against the law.
- You agree that any private motor vehicles, equipment, or personal belongings which you have taken on any assignment is your sole responsibility and that the Company has no liability in the event of theft or damage to such items. You are to abide by the site traffic regulations and parking arrangements at all times.

3.5 KEYS/FOBS/PASSES

You are responsible for any customer keys which you must sign out from the Nominated person/Area at the start of every duty and returned at the end of every duty. In the event that any fob/swipe card/pass or key is lost then it may be your responsibility to make good the loss.

3.5 SITE OPERATIONS FILE

You agree to read, sign, and carry out the Site Operations File on whichever contract you are assigned. Failure to comply with the content of these instructions or customer operating procedures is a disciplinary matter. These instructions are not to be copied without permission from senior management at the Company.

3.6 COMMUNICATIONS BOOK

You are required to maintain a record of events, incidents, accidents, Health & Safety matters, or any unusual occurrences, which occur during your shift period, in the Communication Book. You must report any matter deemed serious or reportable to your Line Manager and the customer as required. The Communication Book must never be completed in advance and all entries must be accurate and factual when reporting this to your Line Manager.

SECTION 03

ICS Cleaning

3.7 CLEANING CUPBOARDS

You must ensure that the cleaning cupboard and the surrounding areas are kept clean and tidy at all times. This includes all facilities which you have used during the course of your duty.

SECTION 04

SPS Group Geneal Rules

This section of the Handbook applies to employees and workers of all companies in the SPS Group. These rules must be read in conjunction with Assignment Instructions, the site operations file and other site instructions, which must be followed at all times. Where these are different to general Company rules, the Assignment Instructions, site operations file and other site instructions should take precedence.

4.1 PROPERTY/ PERSONAL BELONGINGS

- You agree that any private motor vehicles, equipment or personal belongings or property which you have taken to any site or place of work is your sole responsibility and that your employer has no liability in the event of theft or damage to such items.
- You are to abide by the site traffic regulations and parking arrangements at all times, whether in your own or a company vehicle.

4.2 CUSTOMER EQUIPMENT

- You agree that you will not tamper or interfere with any equipment on any assignment/whilst working on any customer site. This includes, but is not limited to, computers, photocopiers, vending machines, telephones, plants, vehicles, electric, gas or water metres or any other equipment.
- In respect of computers, “hacking” is against the law. This includes accessing someone’s internet/email account. You are not permitted access to the internet or the customer’s computers unless authorised by the customer. Staff are not permitted to access any customer or company hardware or software. Unauthorised access to computer material is a disciplinary matter and may in certain cases be a criminal offence. Unauthorised modification of computer material is a criminal offence.
- Using your own personal computer/laptop/tablet or any other media advice on any contract whilst on duty is forbidden unless written authorisation is obtained from the customer/your employer.

SECTION 04

SPS Group Geneal Rules

- Use of the customers or the employer’s internet, including wi-fi, for personal use is strictly prohibited.
- Any breaches of the above rules may result in disciplinary action.

4.3 UNIFORMS

- You must wear issued uniform at all times whilst on duty/at work. This uniform must not be worn in public when you are not on duty apart from travelling to and from work.
- Baseball caps are not permitted headwear whilst on duty unless they are specified as an item of uniform on a specific assignment or contract.

4.4 SMOKING

- You are not permitted to smoke whilst on duty/at work unless there is a designated smoking area.
- You must never smoke whilst on patrol/carrying out your duties or in no smoking areas.
- Where smoke breaks are permitted these are to be kept to the absolute minimum and as dictated in the Assignment Instructions or by your supervisor.
- Smoking is not permitted in any company vehicles.

4.5 ADDRESSING THE CUSTOMER

- You must address customers and their staff, and members of the public you come into contact within the course of your employment, in a courteous manner at all times.

4.6 GROUP POLICIES

- This section of the Handbook applies to employees and workers of all companies in the SPS Group.
- References to the Group, the Company, we/us etc should be interpreted as referring to your employer and any other group company for which you have or may work or perform services.

SECTION 05

Employee Mental Health and Wellbeing

5. Introduction

The SPS Group recognises that supporting the mental wellbeing of our employees is an important for both individuals and the organisation. Mental wellbeing is a key factor in an individual’s health and safety, social wellbeing, and productivity. By promoting good mental health, the positive benefits are realised by individuals, their families, and the broader society. The many different aspects of mental ill-health and stress are associated with a broader range of illnesses and disabilities within our society today.

A positive, supportive culture for mental wellbeing is important for all employees and therefore should be applied across the organisation. Everyone can contribute to mental wellbeing in our workplace and by doing so deliver a wide range of benefits to employees, the organisation, and others. In doing so we can also support those who have experienced mental health problem within the world of work, through better access to employment opportunities and ongoing help and assistance.

5.1 The Purpose of our Mental Health and Wellbeing policy

This policy sets out the framework for our organisation to provide a positive environment that promotes and support a positive state of mental health and wellbeing for our employees and those we work with. The policy also aims to ensure those who are experiencing mental health issues are supported through a number of measures with respect, confidentiality and without discrimination.

5.2 Policy Scope

This policy applies to the entire organisation including employees Where applicable, due consideration should be given to our policy and its goals when dealing with people outside of our organisation.

5.3 Policy Aims

Our organisation plans to implement this policy to achieve the following aims:

- To promote good mental health and wellbeing of all staff through effective communication of our policies and best practice.
- To increase the awareness of our workforce regarding issues associated with mental health and wellbeing and to develop the skills and knowledge of managers, supervisors, and staff to deal with these issues.

SECTION 05

Employee Mental Health and Wellbeing

- To provide support to staff experiencing a mental health problem while in employment and upon return from any absence, whilst preventing discrimination.

5.4 Achieving the Policy Aims

The organisation will promote a culture of good mental health and wellbeing to all staff as follows:

- Through effective communication designed to raise awareness and understanding about mental health and wellbeing.
- By implementing measures at all levels of the organisation that provide a workplace and culture promotes good mental health.
- By listening to our staff and adapting workplace policies (as required) and implementing the policies and evaluating their effectiveness.
- The organisation will provide knowledge and skills training to help management, supervisors and staff support their own mental health and wellbeing and that of others. This training will be designed to address the following:
- The promotion of understanding of the importance of mental wellbeing to all employees, including best practice.
- How to deal with issues around mental health and stress effectively.
- Ensure that any employee suffering from mental illness is treated fairly, with respect and confidentiality and without discrimination.
- Where appropriate, the organisation will train Mental Health First Aiders to support the goals and implementation of this policy.

5.5 Providing support to our staff:

We undertake to provide the following measures and ways of working to promote mental health and wellbeing.

- Offering flexible working arrangements where practicable.
- Working with employees to create a culture where bullying, harassment and discrimination is not accepted.
- Providing training for all employees to raise awareness of everyday contributory factors, such as stress and excessive workload, that undermine mental health.
- Ensuring that managers and supervisory staff are aware of their obligations to promote a good

SECTION 05

Employee Mental Health and Wellbeing

- working environment for their staff and colleagues as defined within this policy.
- Implementing training and awareness programmes to create a culture where staff are able to talk openly about mental health problems and disclose difficulties without fear of discrimination or reprisal.
- Providing proactive support for individual staff who are experiencing mental health problems, inside and outside the workplace, in a positive manner.

5.6 Where an employee is experiencing mental health issues, we will provide support in the following ways:

- Proactively making employees aware of third party organisations that might be able to provide information, advice, and support in these situations.
- Offering continued employment where practicable subject to appropriate adaptations to the role,
- In situations where the staff member experiences a period of absence from work due to mental ill-health, working with the employee to develop a “Return to Work Plan” that provides the best opportunity for the employee to return to work as soon as is reasonably practicable.
- Ensuring that the employee is treated fairly and without discrimination.
- Encouraging staff to seek the appropriate help through the NHS or a mental health support organisation.
- Identifying and remediating any factors within the workplace that are contributing to the negative mental health issues.
- Dealing with the mental health related issues in a sensitive manner, respecting the employee as an individual and acknowledging their right to confidentiality.
- Being mindful of the organisation’s responsibilities under The Equality Act 2010.

5.7 This policy recognises that reducing stress in the workplace is a key component of supporting mental health and wellbeing. Our organisation shall promote the principles and activities below through workforce training and ongoing staff communication.

- Workload demands and expectations placed on employees should be effectively communicated, be achievable and accepted by all parties.
- We will promote an environment where staff are encouraged to feedback to their line management about factors in their job roles that may induce stress, such as excessive workload or overly stretching

SECTION 05

Employee Mental Health and Wellbeing

- performance targets.
- Provide adequate support and training to enable the employee to meet the requirements of their role.
- Provide sufficient communication to keep employees adequately informed about any information that may impact the organisation and their roles.
- Ensure that managers and supervisors are aware of their responsibilities towards their staff, including setting and managing performance in a manner that is consistent with this policy.

5.8 SPS Mental Health & Wellbeing Policy

Responsibilities

Directors:

- Ensure that this policy receives the necessary support and prioritisation to achieve its aim.
- Participate in the annual review of this policy and its effectiveness (See Monitoring and Review)
- Ensure that managers and supervisors are aware of, and implementing, their responsibilities.

Managers and supervisors:

- Ensure that staff are made aware of this policy, at induction and how to access it afterwards.
- Actively promote a culture of good mental health and wellbeing through the implementation of this policy.
- Manage and review the effectiveness of this policy on staff, and feedback to senior leadership as appropriate.

All employees:

- Read and understand this policy, including changes, seeking clarification where required.
- Support our aim of providing a culture of good mental health and wellbeing through their activities and when considering others.
- Take care of their own health and wellbeing, including mental health.
- Ensure that their actions do not affect the health and safety and general wellbeing of other people in the workplace.
- Raise issues or concerns and seek help from their line manager or an appropriate senior manager or Director.

SECTION 05

Employee Mental Health and Wellbeing

5.9 SPS Mental Health & Wellbeing Policy

Communication

We will ensure that all employees receive a copy of this policy during the induction process and have continued access to the policy throughout the length of their employment. Employees should remain informed as the policy changes and be empowered to actively contribute and provide feedback to this policy.

Monitoring and review

We will review this policy annually or more frequently as required, for example to address issues highlighted through employee feedback or to react to legislative changes. The policy should objectively assess whether the stated policy aims have been met and review the effectiveness of the measures within this document.

Effectiveness of the policy will be assessed through:

- Feedback from the workforce, including complaints, appraisals/performance reviews, return to work surveys and exit interviews as appropriate.
- Staff turnover, retirement, and sickness statistics.
- Outcomes of any mental health issues supported through this policy.

Emergency contacts

NHS Medical information and advice - 111

SAMARITANS Emergency telephone number - 116 123

MIND Infoline - 0300 123 3393

SECTION 05

Employee Mental Health and Wellbeing

Useful resources

Anxiety UK - www.anxietyuk.org.uk
ACAS Help and advice - www.acas.org.uk/mentalhealth
NHS Choices (Moodzone) - www.nhs.uk/conditions/stress-anxiety-depression
RETHINK - www.rethink.org
The Mental Health Foundation - www.mentalhealth.org.uk
Workways - www.workways.org.uk
The Equality Act 2010 https://www.legislation.gov.uk/ukpga/2010/15/contents

SECTION 06

Training

6. Introduction

The SPS Group is subject to a variety of statutory regulations, and it must ensure that personnel are trained to levels appropriate to their roles, in order to perform legally and effectively in the best interests of themselves and its customers.

6.1 In order to achieve these aims, the SPS Group undertakes to:

- Identify staff training and development needs in the light of, for example, statutory requirements, necessary standards of competence, innovation, and personal aspirations;
- Set annual priorities in the light of these needs, given budgetary constraints;
- Produce annual costed training and development plans to ensure that these priorities are addressed; Provide appropriate and high-quality induction, training, and development programmes for all staff groups, which may be delivered within assignments or centrally;
- Ensure that all staff are informed of these;
- Monitor and evaluate the effectiveness of induction, training, and development programmes with a view to continued improvement;
- Keep a record of the training received by each member of staff.

6.2 The SPS Group recognises that for its training policy to be effective, those in managerial or supervisory positions must be held accountable for giving their staff constructive, honest, and timely appraisals of their performance and for developing plans for improvement which should consider both the goals of the company and the relevant aspirations of the individual.

6.3 The SPS Group also recognises that for its training policy to be effective, staff must take responsibility for their own development. In addition to undertaking mandatory training required by law, they are expected to avail themselves of the opportunities provided and to make use of training and development to enable them to respond flexibly to change.

SECTION 07

Drug and Alcohol Policy

- 7.1** Drug and alcohol abuse contributes to numerous lost working hours and causes many workplace accidents or injuries every year. Our policy is to employ persons free from alcohol abuse or the use of illegal drugs. The SPS Group takes drug and alcohol abuse from its employees as a serious matter and will not tolerate it. We absolutely prohibit employees using or consuming alcohol or non-prescribed drugs at the workplace or while on company business. We also discourage non-workplace drug and alcohol abuse. The use, sale or possession of alcohol or drugs while at work or on company property will result in disciplinary action, up to and including termination of employment, and may also have legal consequences.
- 7.2** Employees are expected and required to report to work on time and in an appropriate mental and physical state for work. It is our intent and obligation to provide a drug-free, Healthy, and safe work environment for all our staff. We reserve the right to demand a drug or alcohol test of any employee, based upon reasonable suspicion. Reasonable suspicion includes, but is not limited to, physical evidence of use, involvement in an accident, or a substantial drop off in work performance. Failure to take a requested test may lead to discipline, including possible termination.
- 7.3** We also need to exercise caution in relation to prescribed or over-the-counter medication which can affect your workplace performance. You may be suspended if we conclude that you cannot perform your job properly or safely because of using over the counter or prescribed medication. Please inform us prior to working under the influence of a prescribed or over-the-counter medication which may affect your performance.
- 7.4** You must report any conviction under a criminal drug offence for violations occurring on or off any of the Company’s premises. A report of a conviction must be made within 3 days of receipt of a conviction. We will make every effort to assist those who wish to seek treatment or rehabilitation for drug or alcohol dependency. Conscientious efforts to seek such help will not jeopardise any individual employee’s career and any notes on any personnel record will not be used in any decision-making process. If you do have a drug or alcohol problem, please tell us and we may be able to help.

SECTION 08

Equity and Diversity Policy

- 8. EQUAL OPPORTUNITIES STATEMENT**
- 8.1** We are committed to promoting equal opportunities in employment. You and any job applicants will receive equal treatment regardless of age, disability, gender reassignment, marital or civil partner status, pregnancy or maternity, race, colour, nationality, ethnic or national origin, religion or belief, sex, or sexual orientation (Protected Characteristics).
- 8.2. ABOUT THIS POLICY**
- 8.2.1** This policy sets out our approach to equal opportunities and the avoidance of discrimination at work. It applies to all aspects of employment with us, including recruitment, pay and conditions, training, appraisals, promotion, conduct at work, disciplinary and grievance procedures, and termination of employment.
- 8.2.2** This policy does not form part of any employee’s contract of employment, and we may amend it at any time.
- 3.DISCRIMINATION**
- 3.1** You must not unlawfully discriminate against or harass other people including current and former employees, job applicants, clients, customers, suppliers, and visitors. This applies in the workplace, outside the workplace (when dealing with customers, suppliers, or other work-related contacts or when wearing a work uniform), and on work-related trips or events including social events.
- 3.2** The following forms of discrimination are prohibited under this policy and are unlawful:
- (a)** Direct discrimination: treating someone less favourably because of a Protected Characteristic. For example, rejecting a job applicant because of their religious views or because they may have a particular sexual orientation.
 - (b)** Indirect discrimination: a provision, criterion or practice that applies to everyone but adversely affects people with a particular Protected Characteristic more than others and is not justified. For example, requiring a job to be done full-time rather than part-time would adversely affect women because they generally have greater childcare commitments than men. Such a requirement would be discriminatory unless it can be justified.
 - (c)** Harassment: this includes sexual harassment and other unwanted conduct related to a Protected Characteristic, which has the purpose or effect of violating someone’s dignity or creating an intimidating, hostile, degrading, humiliating or offensive environment for them. Harassment is dealt with further in our Anti-harassment and Bullying Policy.

SECTION 08

Equity and Diversity Policy

- (d) Victimisation: retaliation against someone who has complained or has supported someone else’s complaint about discrimination or harassment.
- (e) Disability discrimination: this includes direct and indirect discrimination, any unjustified less favourable treatment because of the effects of a disability, and failure to make reasonable adjustments to alleviate disadvantages caused by a disability.

8.4 RECRUITMENT AND SELECTION

- 8.4.1 Recruitment, promotion, and other selection exercises such as redundancy selection will be conducted on the basis of merit, against objective criteria that avoid discrimination. Shortlisting should be done by more than one person if possible.
- 8.4.2 Vacancies should generally be advertised widely to encourage diversity of applications. Advertisements should avoid stereotyping or using wording that may discourage particular groups from applying.
- 8.4.3 Job applicants should not be asked questions which might suggest an intention to discriminate on grounds of a Protected Characteristic. For example, applicants should not be asked whether they are pregnant or planning to have children.
- 8.4.4 Job applicants should not be asked about health or disability before a job offer is made, except in the very limited circumstances allowed by law: for example, to check that the applicant could perform an intrinsic part of the job (taking account of any reasonable adjustments), or to see if any adjustments might be needed at interview because of a disability. Where necessary, job offers can be made conditional on as satisfactory medical check. Health or disability questions may be included in equal opportunities monitoring forms, which must not be used for selection or decision-making purposes.

8.5 DISABILITIES

- 8.5.1 If you are disabled or become disabled, we encourage you to tell us about your condition so that we can consider what reasonable adjustments or support may be appropriate.

8.6 PART-TIME AND FIXED-TERM WORK

- 8.6.1 Part-time and fixed-term employees should be treated the same as comparable full-time or permanent employees and enjoy no less favourable terms and conditions (on a pro-rata basis where appropriate) unless different treatment is justified.

SECTION 08

Equity and Diversity Policy

8.7 BREACHES OF THIS POLICY

- 8.7.1 We take a strict approach to breaches of this policy, which will be dealt with in accordance with our Disciplinary Procedure. Serious cases of deliberate discrimination may amount to gross misconduct resulting in dismissal.
- 8.7.2 If you believe that you have suffered discrimination you can raise the matter through our Grievance Procedure or Anti-harassment and Bullying Policy. Complaints will be treated in confidence and investigated as appropriate.
- 8.7.3 You must not be victimised or retaliated against for complaining about discrimination. However, making a false allegation deliberately and in bad faith will be treated as misconduct and dealt with under our Disciplinary Procedure.

SECTION 09

Anti-Harrassment and Bullying Policy

9.1 ABOUT THIS POLICY

- 9.1.1 We are committed to providing a working environment free from harassment and bullying and ensuring all staff are treated, and treat others, with dignity and respect.
- 9.1.2 This policy covers harassment or bullying which occurs at work and out of the workplace, such as on business trips or at work-related events or social functions. It covers bullying and harassment by staff (which may include consultants, contractors, and agency workers) and also by third parties such as customers, suppliers, or visitors to our premises.
- 9.1.3 This policy does not form part of any employee’s contract of employment, and we may amend it at any time.

9.2 WHAT IS HARASSMENT?

- 9.2.1 Harassment is any unwanted physical, verbal, or non-verbal conduct that has the purpose or effect of violating a person’s dignity or creating an intimidating, hostile, degrading, humiliating or offensive environment for them. A single incident can amount to harassment.

SECTION 09

Anti-Harrassment and Bullying Policy

- 9.2.2 It also includes treating someone less favourably because they have submitted or refused to submit to such behaviour in the past.
- 9.2.3 Unlawful harassment may involve conduct of a sexual nature (sexual harassment), or it may be related to age, disability, gender reassignment, marital or civil partner status, pregnancy or maternity, race, colour, nationality, ethnic or national origin, religion or belief, sex, or sexual orientation. Harassment is unacceptable even if it does not fall within any of these categories.
- 9.2.4 Harassment may include, for example:
- (a) unwanted physical conduct or “horseplay”, including touching, pinching, pushing, and grabbing;
 - (b) unwelcome sexual advances or suggestive behaviour (which the harasser may perceive as harmless);
 - (c) offensive e-mails, text messages or social media content;
 - (d) mocking, mimicking, or belittling a person’s disability.
- 9.2.5 A person may be harassed even if they were not the intended “target”. For example, a person may be harassed by racist jokes about a different ethnic group if the jokes create an offensive environment.

9.3 WHAT IS BULLYING?

- 9.3.1 Bullying is offensive, intimidating, malicious or insulting behaviour involving the misuse of power that can make a person feel vulnerable, upset, humiliated, undermined or threatened. Power does not always mean being in a position of authority but can include both personal strength and the power to coerce through fear or intimidation.
- 9.3.2 Bullying can take the form of physical, verbal, and non-verbal conduct. Bullying may include, by way of example:
- (a) physical or psychological threats;
 - (b) overbearing and intimidating levels of supervision;
 - (c) inappropriate derogatory remarks about someone’s performance;
- 9.3.3 Legitimate, reasonable, and constructive criticism of a worker’s performance or behaviour, or reasonable instructions given to workers in the course of their employment, will not amount to bullying on their own.

9.4 IF YOU ARE BEING HARASSED OR BULLIED

- 9.4.1 If you are being harassed or bullied, consider whether you feel able to raise the problem informally with the person responsible. You should explain clearly to them that their behaviour is not welcome

SECTION 09

Anti-Harrassment and Bullying Policy

- or makes you uncomfortable. If this is too difficult or embarrassing, you should speak to your line manager or the Health and Safety and Compliance Manager who can provide confidential advice and assistance in resolving the issue formally or informally.
- 9.4.1 If informal steps are not appropriate, or have not been successful, you should raise the matter formally under our Grievance Procedure.
- 9.4.1 We will investigate complaints in a timely and confidential manner. The investigation will be conducted by someone with appropriate experience and no prior involvement in the complaint, where possible. Details of the investigation and the names of the person making the complaint and the person accused must only be disclosed on a “need to know” basis. We will consider whether any steps are necessary to manage any ongoing relationship between you and the person accused during the investigation.
- 9.4.1 Once the investigation is complete, we will inform you of our decision. If we consider you have been harassed or bullied by an employee, the matter will be dealt with under the Disciplinary Procedure as a case of possible misconduct or gross misconduct. If the harasser or bully is a third party such as a customer or other visitor, we will consider what action would be appropriate to deal with the problem. Whether or not your complaint is upheld, we will consider how best to manage any ongoing working relationship between you and the person concerned.

9.5 PROTECTION AND SUPPORT FOR THOSE INVOLVED

- 9.5.1 Staff who make complaints or who participate in good faith in any investigation must not suffer any form of retaliation or victimisation as a result. Anyone found to have retaliated against or victimised someone in this way will be subject to disciplinary action under our Disciplinary Procedure.

9.6 RECORD-KEEPING

- 9.6.1 Information about a complaint by or about an employee may be placed on the employee’s personnel file, along with a record of the outcome and of any notes or other documents compiled during the process. These will be processed in accordance with our Data Protection Policy.

SECTION 10

Anti-Corruption and Bribery Policy

10 ABOUT THIS POLICY

- 10.1.1 It is our policy to conduct all of our business in an honest and ethical manner. We take a zero-tolerance approach to bribery and corruption and are committed to acting professionally, fairly and with integrity in all our business dealings and relationships.
- 10.1.2 Any employee who breaches this policy will face disciplinary action, which could result in dismissal for gross misconduct. Any non-employee who breaches this policy may have their contract terminated with immediate effect.
- 10.1.3 This policy does not form part of any employee’s contract of employment, and we may amend it at any time. It will be reviewed regularly.

10.2 WHO MUST COMPLY WITH THIS POLICY?

- 10.2.1 This policy applies to all persons working for us or on our behalf in any capacity, including employees at all levels, directors, officers, agency workers, seconded workers, volunteers, agents, contractors, external consultants, third-party representatives, and business partners.

10.3 WHAT IS BRIBERY?

- 10.3.1 Bribe means a financial or other inducement or reward for action which is illegal, unethical, a breach of trust or improper in any way. Bribes can take the form of money, gifts, loans, fees, hospitality, services, discounts, the award of a contract or any other advantage or benefit.
- 10.3.2 Bribery includes offering, promising, giving, accepting, or seeking a bribe.
- 10.3.3 All forms of bribery are strictly prohibited. If you are unsure about whether a particular act constitutes bribery, raise it with your line manager or the Health and Safety and Compliance Manager.
- 10.3.4 Specifically, you must not:
 - (a) give or offer any payment, gift, hospitality, or other benefit in the expectation that a business advantage will be received in return, or to reward any business received;
 - (b) accept any offer from a third party that you know, or suspect is made with the expectation that we will provide a business or financial advantage for them or anyone else;
 - (c) give or offer any payment (sometimes called a facilitation payment) to a government official in any country to facilitate or speed up a routine or necessary procedure.

SECTION 10

Anti-Corruption and Bribery Policy

- 10.3.5 You must not threaten or retaliate against another person who has refused to offer or accept a bribe or who has raised concerns about possible bribery or corruption.
- 10.4 GIFTS AND HOSPITALITY
 - 10.4.1 This policy does not prohibit the giving or accepting of reasonable and appropriate hospitality for legitimate purposes such as building relationships, maintaining our image or reputation, or marketing our products and services.
 - 10.4.2 A gift or hospitality will not be appropriate if it is unduly lavish or extravagant or could be seen as an inducement or reward for any preferential treatment (for example, during contractual negotiations or a tender process).
 - 10.4.3 Gifts must be of an appropriate type and value depending on the circumstances and taking account of the reason for the gift. Gifts must not include cash or cash equivalent (such as vouchers) or be given in secret. Gifts must be given in our name, not your name.
 - 10.4.4 Promotional gifts of low value such as branded stationery may be given to or accepted from existing customers, suppliers, and business partners.

10.5 RECORD-KEEPING

- 10.5.1 You must declare and keep a written record of all hospitality or gifts given or received. You must also submit all expenses claims relating to hospitality, gifts, or payments to third parties in accordance with our expenses policy and record the reason for expenditure.
- 10.5.2 All accounts, invoices, and other records relating to dealings with third parties including suppliers and customers should be prepared with strict accuracy and completeness. Accounts must not be kept “off-book” to facilitate or conceal improper payments.

10.6 HOW TO RAISE A CONCERN

- 10.6.1 If you are offered a bribe, or are asked to make one, or if you suspect that any bribery, corruption, or other breach of this policy has occurred or may occur, you must notify your line manager or the Health and Safety and Compliance Manager as soon as possible.

SECTION 11

Whistleblowing Policy

11.1 ABOUT THIS POLICY

- 11.1.1 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.
- 11.1.2 This policy covers all employees, officers, consultants, contractors, casual workers, and agency workers.
- 11.1.3 This policy does not form part of any employee’s contract of employment, and we may amend it at any time.

11.2 What is whistleblowing?

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.

11.3 How to raise a concern

- 11.3.1 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 the Managing Director of your employer. Contact details are at the end of this policy.
- 11.3.2 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.

11.4 Confidentiality

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.

11.5 External disclosures

- 11.5.1 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.

SECTION 11

Whistleblowing Policy

- 11.5.2 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. Protect operates a confidential helpline. Their contact details are at the end of this policy.

11.6 Protection and support for whistle blowers

- 11.6.1 We aim to encourage openness and will support whistle blowers who raise genuine concerns under this policy, even if they turn out to be mistaken.
- 11.6.2 Whistle blowers 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 the appropriate Managing Director immediately.
- 11.6.3 You must not threaten or retaliate against whistle blowers in any way. If you are involved in such conduct, you may be subject to disciplinary action. In some cases, the whistle blower could have a right to sue you personally for compensation in an employment tribunal.
- 11.6.4 However, if we conclude that a whistle blower has made false allegations maliciously, the whistle blower may be subject to disciplinary action.
- 11.6.5 Protect operates a confidential helpline. Their contact details are at the end of this policy.

7 Contacts

7.1 Managing Director

- For SPS Security Limited - John Beharrell – [01482 226570]
- For Independent Cleaning Services Limited – Chris Turner – [01482 226570]

7.2 Protect

- (Independent whistleblowing charity)
- Helpline: 0203 117 2520
- E-mail: whistle@pcaw.co.uk
- Website: www.pcaw.co.uk

SECTION 12

IT and Communications Systems Policy

12.1 ABOUT THIS POLICY

- 12.1.1 Our IT and communications systems are intended to promote effective communication and working practices. This policy outlines the standards you must observe when using these systems, when we will monitor their use, and the action we will take if you breach these standards.
- 12.2.1 Breach of this policy may be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.
- 12.3.1 This policy does not form part of any employee’s contract of employment, and we may amend it at any time.

12.2 EQUIPMENT SECURITY AND PASSWORDS

- 12.2.1 You are responsible for the security of the equipment allocated to or used by you, and you must not allow it to be used by anyone other than in accordance with this policy. You should use passwords on all IT equipment, particularly items that you take out of the office. You should keep your passwords confidential and change them regularly.
- 12.2.1 You must only log on to our systems using your own username and password. You must not use another person’s username and password or allow anyone else to log on using your username and password.
- 12.2.1 If you are away from your desk, you should log out or lock your computer. You must log out and shut down your computer at the end of each working day.

12.3 SYSTEMS AND DATA SECURITY

- 12.3.1 You should not delete, destroy, or modify existing systems, programs, information, or data (except as authorised in the proper performance of your duties).
- 12.3.2 You must not download or install software from external sources without authorisation from a Company Director. Downloading unauthorised software may interfere with our systems and may introduce viruses or other malware.
- 12.3.3 You must not attach any device or equipment including mobile phones, tablet computers or USB storage devices to our systems without authorisation from a Company Director
- 12.3.4 We monitor all e-mails passing through our system for viruses. You should exercise particular caution when opening unsolicited e-mails from unknown sources. If an email looks suspicious do not reply to it, open any attachments, or click any links in it.
- 12.3.5 Inform Jupiter IT immediately if you suspect your computer may have a virus.

SECTION 12

IT and Communications Systems Policy

12.4 EMAIL

- 12.4.1 Adopt a professional tone and observe appropriate etiquette when communicating with third parties by email.
- 12.4.2 Remember that emails can be used in legal proceedings and that even deleted e-mails may remain on the system and be capable of being retrieved.
- 12.4.3 You must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic, or otherwise inappropriate e-mails.
- 12.4.4 You should not:
 - (a) send or forward private e-mails at work which you would not want a third party to read;
 - (b) send or forward chain mail, junk mail, cartoons, jokes, or gossip;
 - (c) contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding e-mails to others who do not have a real need to receive them; or
 - (d) send messages from another person’s e-mail address (unless authorised) or under an assume name.
- 12.4.5 Do not use your own personal e-mail account to send or receive e-mail for the purposes of our business. Only use the e-mail account we have provided for you.
- 12.4.6 [We do not permit access to web-based personal e-mail such as Gmail or Hotmail on our computer systems at any time due to additional security risks.]

12.5 USING THE INTERNET

- 12.5.1 Internet access is provided [primarily OR solely] for business purposes. [Occasional personal use may be permitted as set out in paragraph 6.
- 12.4.2 You should not access any web page or download any image or other file from the internet which could be regarded as illegal, offensive, in bad taste or immoral. Even web content that is legal in the UK may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.
- 12.4.3 We may block or restrict access to some websites at our discretion.

12.6 PERSONAL USE OF OUR SYSTEMS

- 12.6.1 We permit the incidental use of our systems to send personal e-mail, browse the internet and make personal telephone calls subject to certain conditions. Personal use is a privilege and not a right. It

SECTION 12

IT and Communications Systems Policy

must not be overused or abused. We may withdraw permission for it at any time or restrict access at our discretion.

12.6.2 Personal use must meet the following conditions:

- (a) it must be minimal and take place exclusively outside of normal working hours (that is, during breaks, and before or after work);
- (b) personal e-mails should be labelled “personal” in the subject header;
- (c) it must not affect your work or interfere with the business
- (d) it must not commit us to any marginal costs; and
- (e) it must comply with our policies including the Equal Opportunities Policy, Anti-harassment and Bullying Policy, Data Protection Policy, and Disciplinary Procedure.

12.7 MONITORING

12.7.1 Our systems enable us to monitor telephone, e-mail, voicemail, internet, and other communications. For business reasons, and in order to carry out legal obligations in our role as an employer, your use of our systems including the telephone and computer systems (including any personal use) may be continually monitored by automated software or otherwise.

- 12.7.1 We reserve the right to retrieve the contents of e-mail messages or check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the business, including for the following purposes (this list is not exhaustive):
- (a) to monitor whether the use of the e-mail system or the internet is legitimate and in accordance with this policy;
 - (b) to find lost messages or to retrieve messages lost due to computer failure;
 - (c) to assist in the investigation of alleged wrongdoing; or
 - (d) to comply with any legal obligation.

12.8 PROHIBITED USE OF OUR SYSTEMS

- 12.8.1 Misuse or excessive personal use of our telephone or e-mail system or inappropriate internet use will be dealt with under our Disciplinary Procedure. Misuse of the internet can in some cases be a criminal offence.
- 12.8.2 Creating, viewing, accessing, transmitting, or downloading any of the following material will usually amount to gross misconduct (this list is not exhaustive):

SECTION 12

IT and Communications Systems Policy

- (a) pornographic material (that is, writing, pictures, films, and video clips of a sexually explicit or arousing nature);
- (b) offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or to our clients;
- (c) a false and defamatory statement about any person or organisation;
- (d) material, which is discriminatory, offensive, derogatory or may cause embarrassment to others (including material which breaches our Equal Opportunities Policy or our Anti-harassment and Bullying Policy);
- (e) confidential information about us or any of our staff or clients (except as authorised in the proper performance of your duties);
- (f) unauthorised software;
- (g) any other statement which is likely to create any criminal or civil liability (for you or us); or
- (h) music or video files or other material in breach of copyright.

SECTION 13

Social Media Policy

13.1 ABOUT THIS POLICY

- 13.1.1 This policy is in place to minimise the risks to our business through use of social media.
- 13.1.2 This policy deals with the use of all forms of social media, including Facebook, LinkedIn, Twitter, Instagram, Wikipedia, Snapchat and all other social networking sites, internet postings and blogs. It applies to use of social media for business purposes as well as personal use that may affect our business in any way.
- 13.1.3 This policy does not form part of any employee’s contract of employment, and we may amend it at any time.

13.2 PERSONAL USE OF SOCIAL MEDIA

Occasional personal use of social media during working hours is permitted so long as it does not involve unprofessional or inappropriate content, does not interfere with your employment responsibilities or productivity, and complies with this policy.

SECTION 13

Social Media Policy

13.3 PROHIBITED USE

- 13.3.1 You must avoid making any social media communications that could damage our business interests or reputation, even indirectly.
- 13.3.2 You must not use social media to defame or disparage us, our staff or any third party; to harass, bully or unlawfully discriminate against staff or third parties; to make false or misleading statements; or to impersonate colleagues or third parties.
- 13.3.3 You must not express opinions on our behalf via social media, unless expressly authorised to do so by your manager. You may be required to undergo training in order to obtain such authorisation.
- 13.3.4 You must not post comments about sensitive business-related topics, such as our performance, or do anything to jeopardise our trade secrets, confidential information, and intellectual property. You must not include our logos or other trademarks in any social media posting or in your profile on any social media.

The contact details of business contacts made during the course of your employment are our confidential information. On termination of employment, you must provide us with a copy of all such information, delete all such information from your personal social networking accounts and destroy any further copies of such information that you may have.
- 13.3.5 Any misuse of social media should be reported to Managing Director

13.4 GUIDELINES FOR RESPONSIBLE USE OF SOCIAL MEDIA

- 13.4.1 You should make it clear in social media postings, or in your personal profile, that you are speaking on your own behalf. Write in the first person and use a personal e-mail address.
- 13.4.2 Be respectful to others when making any statement on social media and be aware that you are personally responsible for all communications which will be published on the internet for anyone to see.
- 13.4.3 If you disclose your affiliation with us on your profile or in any social media postings, you must state that your views do not represent those of your employer (unless you have been authorised to speak on our behalf as set out in paragraph 3.3). You should also ensure that your profile and any content you post are consistent with the professional image you present to clients and colleagues.
- 13.4.4 If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from posting it until you have discussed it with your manager.
- 13.4.5 If you see social media content that disparages or reflects poorly on us, you should contact your manager.

SECTION 13

Social Media Policy

13.5 BREACH OF THIS POLICY

- 13.5.1 Breach of this policy may result in disciplinary action up to and including dismissal.
- 13.6.1 You may be required to remove any social media content that we consider to constitute a breach of this policy. Failure to comply with such a request may result in disciplinary action.

SECTION 14

Data Privacy Notice for Employees, Workers, and Contractors

14.1 INTRODUCTION

- 14.1.1 We are committed to protecting the privacy and security of your personal information.
- 14.1.2 This privacy notice describes how we collect and use personal information about you during and after your working relationship with us, in accordance with the UK General Data Protection Regulation (UK GDPR).
- 14.1.3 It applies to all employees, workers, and contractors. Your employer is a “controller”. This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.
- 14.1.4 This notice applies to current and former employees, workers, and contractors. This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time but if we do so, we will provide you with an updated copy of this notice as soon as reasonably practical.
- 14.15 It is important that you read and retain this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information and what your rights are under the data protection legislation.

SECTION 14

Data Privacy Notice for Employees, Workers, and Contractors

14.2 DATA PROTECTION PRINCIPLES

We will comply with data protection law. This says that the personal information we hold about you must be:

- 14.2.1 Used lawfully, fairly and in a transparent way.
- 14.2.2 Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- 14.2.3 Relevant to the purposes we have told you about and limited only to those purposes.
- 14.2.4 Accurate and kept up to date.
- 14.2.5 Kept only as long as necessary for the purposes we have told you about.
- 14.2.6 Kept securely.

14.3 THE KIND OF INFORMATION WE HOLD ABOUT YOU

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data). There are certain types of more sensitive personal data which require a higher level of protection, such as information about a person’s health or sexual orientation. Information about criminal convictions also warrants this higher level of protection.

14.3.1 We will collect, store, and use the following categories of personal information about you:

- (a) Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- (b) Date of birth, Gender, Marital status, and dependants, Next of kin and emergency contact information, National Insurance number.
- (c) Bank account details, payroll records and tax status information.
- (d) Salary, annual leave, pension, and benefits information
- (e) Start date and, if different, the date of your continuous employment.
- (f) Leaving date and your reason for leaving.
- (g) Location of employment or workplace.
- (h) Copy of driving licence and other licences and qualifications relevant to your job role.
- (i) Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process)
- (j) Employment records (including job titles, work history, working hours, holidays, training records and professional memberships).

SECTION 14

Data Privacy Notice for Employees, Workers, and Contractors

- (k) Performance information.
- (l) Disciplinary and grievance information.
- (m) CCTV footage and other information obtained through electronic means such as swipe card records and Time gate records.
- (n) Information about your use of our IT systems.
- (o) Photographs.
- 14.3.2 We may also collect, store, and use the following more sensitive types of personal information:
 - (a) Information about your race or ethnicity, religious beliefs, sexual orientation, and political opinions.
 - (b) Trade union membership.
 - (c) Information about your health, including any medical condition, health, and sickness records, including:
 - (d) where you leave employment and under any share plan operated by a group company the reason for leaving is determined to be ill-health, injury or disability, the records relating to that decision;
 - (e) details of any absences (other than holidays) from work including time on statutory parental leave and sick leave; and
 - (f) where you leave employment and the reason for leaving is related to your health, information about that condition needed for pensions and health insurance purposes.
 - (g) Genetic information and biometric data.
 - (h) Information about criminal convictions and offences.

14.4 HOW IS YOUR PERSONAL INFORMATION COLLECTED?

- 14.4.1 We collect personal information about employees, workers and contactors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, credit reference agencies or other background check agencies.
- 14.4.2 We will collect additional personal information in the course of job-related activities throughout the period of you working for us.

SECTION 14

Data Privacy Notice for Employees, Workers, and Contractors

14.5 HOW WE WILL USE INFORMATION ABOUT YOU

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

- 1. Where we need to perform the contract, we have entered into with you.
- 2. Where we need to comply with a legal obligation.
- 3. Where it is necessary for legitimate interests pursued by us or a third party and your interests and fundamental rights do not override those interests.

We may also use your personal information in the following situations, which are likely to be rare:

- 1. Where we need to protect your interests (or someone else’s interests).
- 2. Where it is needed in the public interest.

14.6 SITUATIONS IN WHICH WE WILL USE YOUR PERSONAL INFORMATION

14.6.1 We need all the categories of information in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal obligations. In some cases, we may use your personal information to pursue legitimate interests, provided your interests and fundamental rights do not override those interests. The situations in which we will process your personal information are listed below.

- (a) Making a decision about your recruitment or appointment.
- (b) Determining the terms on which you work for us.
- (c) Checking you are legally entitled to work in the UK.
- (d) Paying you and, if you are an employee or deemed employee for tax purposes, deducting tax and National Insurance contributions (NICs).
- (e) Providing benefits to you, such as a pension.
- (f) Administering the contract, we have entered into with you.
- (g) Business management and planning, including accounting and auditing.
- (h) Conducting performance reviews, managing performance, and determining performance requirements.
- (i) Making decisions about salary reviews.
- (j) Assessing qualifications for a particular job or task, including decisions about promotions.
- (k) Gathering evidence for possible grievance or disciplinary hearings.

SECTION 14

Data Privacy Notice for Employees, Workers, and Contractors

- (l) Making decisions about your continued employment or engagement.
- (m) Making arrangements for the termination of our working relationship.
- (n) Education, training, and development requirements.
- (o) Dealing with legal disputes involving you, or other employees, workers, and contractors, including accidents at work.
- (p) Ascertaining your fitness to work.
- (q) Managing sickness absence.
- (r) Complying with health and safety obligations.
- (s) To prevent fraud.
- (t) To monitor your use of our IT systems to ensure compliance with our IT policies.
- (u) To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- (v) Equal opportunities monitoring.

14.6.2 Some of the lawful grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

14.7 IF YOU FAIL TO PROVIDE PERSONAL INFORMATION

14.7.1 If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

14.8 CHANGE OF PURPOSE

14.8.1 We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

14.8.2 Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

SECTION 14

Data Privacy Notice for Employees, Workers, and Contractors

14.9 HOW WE USE PARTICULARLY SENSITIVE PERSONAL INFORMATION

“Special categories” of particularly sensitive personal information, such as information about your health, racial or ethnic origin, sexual orientation, or trade union membership, require higher levels of protection. We need to have further justification for collecting, storing, and using this type of personal information. We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data. We may process special categories of personal information in the following circumstances:

- 1. In limited circumstances, with your explicit written consent.
 - 2. Where we need to carry out our legal obligations or exercise rights in connection with employment.
 - 3. Where it is needed in the public interest, such as for equal opportunities monitoring.
- Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else’s interests) and you are not capable of giving your consent, or where you have already made the information public.

14.10 SITUATIONS IN WHICH WE WILL USE YOUR SENSITIVE PERSONAL INFORMATION

14.10.1 In general, we will not process particularly sensitive personal information about you unless it is necessary for performing or exercising obligations or rights in connection with employment. On rare occasions, there may be other reasons for processing, such as it is in the public interest to do so. The situations in which we will process your particularly sensitive personal information are listed below.

- (a)** We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits including statutory maternity pay, statutory sick pay, pensions, and permanent health insurance.
- (b)** We will use information about your race or national or ethnic origin, religious, philosophical, or moral beliefs, or your sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.
- (c)** We will use trade union membership information to pay trade union premiums, register the status of a protected employee and to comply with employment law obligations.

SECTION 14

Data Privacy Notice for Employees, Workers, and Contractors

14.11 DO WE NEED YOUR CONSENT?

14.11.1 We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

14.12 INFORMATION ABOUT CRIMINAL CONVICTIONS

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided, we do so in line with our data protection policy.

14.12.1 We envisage that we will hold information about criminal convictions.

14.12.2 We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us. We will use information about criminal convictions and offences in order to determine suitability or employment and continued employment and to comply with any legal requirements.

14.12.3 We are allowed to use your personal information in this way to carry out our obligations in respect of safeguarding and vetting.

14.13 AUTOMATED DECISION-MAKING

14.13.1 Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention.

14.13.2 We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

SECTION 14

Data Privacy Notice for Employees, Workers, and Contractors

14.14 DATA SHARING

We may have to share your data with third parties, including third-party service providers and other entities in our group. We require third parties to respect the security of your data and to treat it in accordance with the law.

14.15 WHY MIGHT YOU SHARE MY PERSONAL INFORMATION WITH THIRD PARTIES?

14.15.1 We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

16 WHICH THIRD-PARTY SERVICE PROVIDERS PROCESS MY PERSONAL INFORMATION?

14.16.1 “Third parties” includes third-party service providers (including contractors and designated agents) and other entities within our group. The following activities are carried out by third-party service providers: payroll, pension administration, benefits provision and administration, IT services, legal services, auditors and administrators of our time and attendance systems.

17 HOW SECURE IS MY INFORMATION WITH THIRD-PARTY SERVICE PROVIDERS AND OTHER ENTITIES IN OUR GROUP?

14.17.1 All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

18 WHEN MIGHT YOU SHARE MY PERSONAL INFORMATION WITH OTHER ENTITIES IN THE GROUP?

14.18.1 We will share your personal information with other entities in our group as part of our regular reporting activities on company performance, in the context of a business reorganisation or group restructuring exercise, for system maintenance support and hosting of data.

14.19 WHAT ABOUT OTHER THIRD PARTIES?

14.19.1 We may share your personal information with other third parties, for example in the context of the possible sale or restructuring of the business or a contracting in or our situation which falls under

SECTION 14

Data Privacy Notice for Employees, Workers, and Contractors

the TUPE Regulations. In this situation we will, so far as possible, share anonymised data with the other parties. Otherwise, we will share your personal data with the other parties if and to the extent required under the terms of the transaction and/or by law.

14.19.2 We may also need to share your personal information with a regulator or to otherwise comply with the law. This may include making returns to HMRC.

14.20 DATA SECURITY

14.20.1 We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used, or accessed in an unauthorised way, altered, or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions, and they are subject to a duty of confidentiality.

14.20.2 We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

DATA RETENTION

14.21 HOW LONG WILL YOU USE MY INFORMATION FOR?

14.21.1 We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

14.22.2 In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker, or contractor of the company we will retain and securely destroy your personal information in accordance with applicable laws and regulations.

SECTION 14

Data Privacy Notice for Employees, Workers, and Contractors

14.23 RIGHTS OF ACCESS, CORRECTION, ERASURE, AND RESTRICTION
YOUR DUTY TO INFORM US OF CHANGES

14.23.1 It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

YOUR RIGHTS IN CONNECTION WITH PERSONAL INFORMATION

- 14.23.1 Under certain circumstances, by law you have the right to:
- (a) Request access to your personal information (commonly known as a “data subject access request”). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
 - (b) Request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
 - (c) Request erasure of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
 - (d) Object to processing of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
 - (e) Request the restriction of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
 - (f) Request the transfer of your personal information to another party.

14.23.3 If you want to review, verify, correct, or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the SPS Group Project & Compliance Manager in writing.

14.24 NO FEE USUALLY REQUIRED

14.24.1 You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

SECTION 14

Data Privacy Notice for Employees, Workers, and Contractors

14.25 WHAT WE MAY NEED FROM YOU

14.25.1 We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

14.26 RIGHT TO WITHDRAW CONSENT

14.26.1 In the limited circumstances where you may have provided your consent to the collection, processing, and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Data Protection Officer. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

14.27 DATA PROTECTION OFFICER

14.27.1 We have appointed a data protection officer (DPO) (contact details below) to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact the DPO.

14.28 CHANGES TO THIS PRIVACY NOTICE

14.28.1 We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

14.29 DPO

14.29.1 The DPO is Jack Tolson who can be contacted as follows:
JACK TOLSON
SPS Group Project & Compliance Manager
Jack.tolson@sps-group.net

SECTION 15

Data Protection Policy

Please see the glossary at the end of this policy which explains the terms used in this Policy. Defined terms that are explained in the glossary begin with a capital letter.

15.1 INTRODUCTION

- a) This Policy sets out how we handle the Personal Data of our customers, suppliers, employees, workers and other third parties.
- b) This Policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.
- c) This Policy applies to all employees, workers, contractors, and directors (" you", "your"). You must read, understand, and comply with this Policy when Processing Personal Data on our behalf and attend training on its requirements. This Policy sets out what we expect from you in order for the Company to comply with applicable law. Your compliance with this Policy is mandatory. Any breach of this Policy may result in disciplinary action.
- d) This Policy (together with any related policies and guidelines) is an internal document and cannot be shared with third parties, clients, or regulators without prior authorisation from the Company's DPO/DPM.

15.2 SCOPE

- a) The DPO/DPM is responsible for overseeing this Policy and, as applicable, developing related policies and guidelines. Please see page 38 for the DPO's contact details.
- b) Please contact the DPO/DPM with any questions about the operation of this Policy or the GDPR or if you have any concerns that this Policy is not being or has not been followed. In particular, you must always contact the DPO/DPM in the following circumstances (which is not an exhaustive list):
 - i) If you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by the Company) (see Section 4 below);
 - ii) If you are unsure about the retention period for any Personal Data (see Section 8 below);
 - iii) If you are unsure about what security or other measures you need to implement to protect Personal Data (see Section 9 below);
 - iv) If there has been a Personal Data Breach (Sections 9 and 10 below);
 - v) If you need any assistance dealing with any rights invoked by a Data Subject (see Section 12);

SECTION 15

Data Protection Policy

- vi) Whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA (see Section 16 below) or plan to use Personal Data for purposes others than what it was collected for.
- vii) If you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making (see Section 17 below);
- viii) If you need help complying with applicable law when carrying out direct marketing activities (see Section 18 below); or
- ix) If you need help with any contracts or other areas in relation to sharing Personal Data with third parties (see Section 19 below).

15.3 PERSONAL DATA PROTECTION PRINCIPLES

- a) We adhere to the principles relating to Processing of Personal Data set out in the GDPR which require Personal Data to be:
 - i) Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).
 - ii) Collected only for specified, explicit and legitimate purposes (Purpose Limitation).
 - iii) Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation).
 - iv) Accurate and where necessary kept up to date (Accuracy).
 - v) Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation).
 - vi) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction, or damage (Security, Integrity, and Confidentiality).
 - vii) Not transferred to another country without appropriate safeguards being in place (Transfer Limitation).
 - viii) Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).
- b) We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

SECTION 15

Data Protection Policy

15.4 LAWFULNESS, FAIRNESS, TRANSPARENCY

a) LAWFULNESS AND FAIRNESS

- i) Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.
- ii) You may only collect, Process, and share Personal Data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

iii) The GDPR allows Processing for specific purposes, some of which are set out below:

- (1) The Data Subject has given his or her Consent;
- (2) The Processing is necessary for the performance of a contract with the Data Subject;
- (3) To meet our legal compliance obligations;
- (4) To protect the Data Subject’s vital interests;
- (5) To pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices or Fair Processing Notices.

iv) We must identify and document the legal ground being relied on for each Processing activity.

b) CONSENT

- i) A Data Controller must only process Personal Data on the basis of one or more of the lawful bases set out in the GDPR, which include Consent.
- ii) A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

SECTION 15

Data Protection Policy

iii) Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

iv) Unless we can rely on another legal basis of Processing, Explicit Consent is usually required for Processing Sensitive Personal Data, for Automated Decision-Making and for cross border data transfers. Usually, we will be relying on another legal basis (and not require Explicit Consent) to Process most types of Sensitive Data. Where Explicit Consent is required, you must issue a Fair Processing Notice to the Data Subject to capture Explicit Consent.

v) You will need to evidence Consent captured and keep records of all Consents so that the Company can demonstrate compliance with Consent requirements.

c) TRANSPARENCY (NOTIFYING DATA SUBJECTS)

i) The GDPR requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices or Fair Processing Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

ii) Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we must provide the Data Subject with all the information required by the GDPR including the identity of the Data Controller and DPO/DPM, how and why we will use, Process, disclose, protect, and retain that Personal Data through a Fair Processing Notice which must be presented when the Data Subject first provides the Personal Data.

iii) When Personal Data is collected indirectly (for example, from a third party or publicly available source), you must provide the Data Subject with all the information required by the GDPR as soon as possible after collecting/receiving the data. You must also check that the Personal Data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

SECTION 15

Data Protection Policy

iv) You must use the Company’s standard Privacy Notices/Fair Processing Notices if you are required to issue these documents in the course of carrying out your role. If you are unsure as to which document to use, you should contact the DPO/DPM.

15.5 PURPOSE LIMITATION

- a) Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.
- b) You cannot use Personal Data for new, different, or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

15.6 DATA MINIMISATION

- a) Personal Data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is Processed.
- b) You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties.
- c) You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.
- d) You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Company’s data retention guidelines.

15.7 ACCURACY

- a) Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

SECTION 15

Data Protection Policy

- b) Where your role involves Processing you should ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards and take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

15.8 STORAGE LIMITATION

- a) Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.
- b) You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.
- c) The Company will ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held unless a law requires such data to be kept for a minimum time. You must comply with the Company’s guidelines on Data Retention.
- d) Where your role involves Processing you should: -
 - i) Take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the Company’s applicable records retention schedules and policies. This includes requiring third parties to delete such data where applicable; and
 - ii) Ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice or Fair Processing Notice.

15.9 SECURITY INTEGRITY AND CONFIDENTIALITY

a) PROTECTING PERSONAL DATA

SECTION 15

Data Protection Policy

- i) Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction, or damage.
- ii) We will develop, implement, and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks. This may include, but is not limited to, data security measures such as password protection, encryption, restrictions on storage of data on certain devices and restrictions on who can access certain areas of our computer systems or physical areas of our premises.
- iii) All employees, workers, contractors, and directors are responsible for protecting the Personal Data we hold and must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.
- iv) You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.
- v) You must maintain data security by protecting the confidentiality, integrity, and availability of the Personal Data, defined as follows:
 - (1) Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it.
 - (2) Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.
 - (3) Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.
- vi) You must comply with and not attempt to circumvent the safeguards we implement in order to protect Personal Data.

SECTION 15

Data Protection Policy

- 15.10 REPORTING A PERSONAL DATA BREACH**
- a) The GDPR requires Data Controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject.
 - b) We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.
 - c) If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the DPO. You should preserve all evidence relating to the potential Personal Data Breach.
- 15.11 TRANSFER LIMITATION**
- a) Due to the special conditions which apply to the transfer of personal data outside the EEA you must refer to the DPO/DPM before carrying out any such transfer.
- 15.12 DATA SUBJECT’S RIGHTS AND REQUESTS**
- a) Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:
 - i) Withdraw Consent to Processing at any time;
 - ii) Receive certain information about the Data Controller’s Processing activities;
 - iii) Request access to their Personal Data that we hold;
 - iv) Prevent our use of their Personal Data for direct marketing purposes;
 - v) Ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;
 - vi) Restrict Processing in specific circumstances;
 - vii) Challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;
 - viii) Request a copy of an agreement under which Personal Data is transferred outside of the EEA;

SECTION 15

Data Protection Policy

- ix) Object to decisions based solely on Automated Processing, including profiling (ADM);
 - x) Prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;
 - xi) Be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
 - xii) Make a complaint to the supervisory authority; and
 - xiii) In limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.
- b) You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).
- c) You must immediately forward any Data Subject request you receive to the DPO.

15.13 ACCOUNTABILITY

- a) As a Data Controller the Company must have adequate resources and controls in place to ensure and to document GDPR compliance.

15.14 RECORD KEEPING

- a) The GDPR requires us to keep full and accurate records of all our data Processing activities.
- b) Where your role involves Processing you should maintain accurate records reflecting our Processing including records of Data Subjects’ Consents and procedures for obtaining Consents in accordance with the Company’s guidelines.

15.15 TRAINING AND AUDIT

- a) You must undergo all mandatory data privacy related training as required by the Company and (for managers and supervisors) ensure your team undergo similar mandatory training.

SECTION 15

Data Protection Policy

15.16 DIRECT MARKETING

- a) We are subject to certain rules and privacy laws when marketing to our customers.
- b) You must comply with any Company guidelines in place in relation to direct marketing to customers.

15.17 SHARING PERSONAL DATA

- a) Generally, we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.
- b) You may only share the Personal Data we hold with another employee, agent, or representative of any of our group companies if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.
- c) You may only share the Personal Data we hold with third parties such as our service providers if:
- i) They have a need to know the information for the purposes of providing the contracted services;
 - ii) Sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject’s Consent has been obtained.
 - iii) The third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
 - iv) The transfer complies with any applicable cross border transfer restrictions; and
 - v) A fully executed written contract that contains GDPR approved third party clauses has been obtained.

15.18 CHANGES TO THIS POLICY

We reserve the right to change this Policy at any time without notice to you so please check regularly to obtain the latest copy of this Policy.

SECTION 16

Disciplinary and Capability Procedure

16.1 ABOUT THIS PROCEDURE

- 16.1.1 This procedure is intended to help maintain standards of conduct and performance and to ensure fairness and consistency when dealing with allegations of misconduct or poor performance.
- 16.1.2 Minor conduct or performance issues can usually be resolved informally with your line manager. This procedure sets out formal steps to be taken if the matter is more serious or cannot be resolved informally.
- 16.1.3 This procedure does not form part of any employee’s contract of employment, and we may amend it or disapply it at any time. We reserve the right not to follow the procedure in full or at all for employees with short service and/or who are under probation or assessment.

16.2 INVESTIGATIONS

- 16.2.1 Before any disciplinary hearing is held, the matter will be investigated. Any meetings and discussions as part of an investigation are solely for the purpose of fact-finding and no disciplinary action will be taken without a disciplinary hearing.
- 16.2.2 In some cases of alleged misconduct, we may need to suspend you from work while we carry out the investigation or disciplinary procedure (or both). While suspended, you should not visit our premises or any of our customers and you should not contact any of our clients, customers, suppliers, contractors, or staff, unless authorised to do so. Suspension is not considered to be disciplinary action.

16.3 THE HEARING

- 16.3.1 We will give you written notice of the hearing, including sufficient information about the alleged misconduct or poor performance and its possible consequences to enable you to prepare. You will normally be given copies of relevant documents and witness statements.
- 16.3.2 You may be accompanied at the hearing by a trade union representative or a colleague, who will be allowed reasonable paid time off to act as your companion.
- 16.3.3 You should let us know as early as possible if there were any relevant witnesses you would like to attend the hearing or any documents or other evidence you wish to be considered.
- 16.3.4 We will inform you in writing of our decision, usually within 7 days of the hearing unless there are reasonable grounds for extending this period.

SECTION 16

Disciplinary and Capability Procedure

16.4 DISCIPLINARY ACTION AND DISMISSAL

- 16.4.1 The usual penalties for misconduct or poor performance are:
 - (a) Stage 1: First written warning. Where there are no other active written warnings on your disciplinary record, you will usually receive a first written warning. It will usually remain active for six months.
 - (b) Stage 2: Final written warning. In case of further misconduct or failure to improve where there is an active first written warning on your record, you will usually receive a final written warning. This may also be used without a first written warning for serious cases of misconduct or poor performance. The warning will usually remain active for 12 months.
 - (c) Stage 3: Dismissal or other action. You may be dismissed for further misconduct or failure to improve where there is an active final written warning on your record, or for any act of gross misconduct. Examples of gross misconduct are given below (paragraph 6).

We may consider other sanctions short of dismissal, including demotion or redeployment to another role (where permitted by your contract), and/or extension of a final written warning with a further review period.

16.5 APPEALS

- 16.5.1 You may appeal in writing within one week of being told of the decision.
- 16.5.2 The appeal hearing will, where possible, be held by someone senior to the person who held the original hearing. You may bring a colleague or trade union representative with you to the appeal hearing.
- 16.5.3 We will inform you in writing of our final decision as soon as possible, usually within one week of the appeal hearing unless there are reasonable grounds for extending this period. There is no further right of appeal.

16.6 GROSS MISCONDUCT

- 16.6.1 Gross misconduct will usually result in dismissal without warning, with no notice or payment in lieu of notice (summary dismissal).
- 16.6.2 Gross misconduct is a serious breach of contract and includes misconduct which, in our opinion, is likely to prejudice our business or reputation or irreparably damage the working relationship

SECTION 16

Disciplinary and Capability Procedure

and trust between us. This may include misconduct committed outside of work. The following are examples of matters that are normally regarded as gross misconduct:

- (a) Theft or fraud;
- (b) Removal of the employer’s or customer’s property without consent (whether temporarily or permanently);
- (c) Physical violence or bullying;
- (d) Deliberate and serious damage to property;
- (e) Serious misuse of the organisation’s property or name;
- (f) Deliberately accessing internet sites containing pornographic, offensive, or obscene material;
- (g) Serious insubordination;
- (h) Unlawful discrimination, victimisation, or harassment;
- (i) Bringing the organisation into serious disrepute;
- (j) Serious incapability at work brought on by alcohol or illegal drugs;
- (k) Causing loss, damage, or injury through serious negligence;
- (l) A serious breach of health and safety rules;
- (m) A serious breach of confidence.

16.6.3 This list is intended as a guide and is not exhaustive.

SECTION 17

Grievance Procedure

17.1 ABOUT THIS PROCEDURE

- 17.1.1 Most grievances can be resolved quickly and informally through discussion with your line manager. If this does not resolve the problem, you should initiate the formal procedure set out below.
- 17.1.2 This procedure applies to employees. It does not apply to agency workers or self-employed contractors.
- 17.1.3 This procedure does not form part of any employee’s contract of employment. It may be amended at any time, and we may depart from it depending on the circumstances of any case.

SECTION 17

Grievance Procedure

17.2 STEP 1: WRITTEN GRIEVANCE

- 17.2.1 You should put your grievance in writing and submit it to your line manager. If your grievance concerns your line manager, you may submit it to a Director.
- 17.2.2 The written grievance should set out the nature of the complaint, including any relevant facts, dates, and names of individuals involved so that we can investigate it.

17.3 STEP 2: MEETING

- 17.3.1 We will arrange a grievance meeting as soon as reasonably possible upon receipt of your written grievance. You should make every effort to attend.
- 17.3.2 You may bring a companion to the grievance meeting if you make a reasonable request in advance and tell us the name of your chosen companion. The companion may be either a trade union representative or a colleague, who will be allowed reasonable paid time off from duties to act as your companion.
- 17.3.3 If you or your companion cannot attend at the time specified you should let us know as soon as possible and we will try, within reason, to agree an alternative time.
- 17. 3.4 We may adjourn the meeting if we need to carry out further investigations, after which the meeting will usually be reconvened.
- 17.3.5 We will write to you, usually within one week of the last grievance meeting (unless there are reasonable grounds for extending this period), to confirm our decision and notify you of any further action that we intend to take to resolve the grievance. We will also advise you of your right of appeal.

17.4 STEP 3: APPEALS

- 17.4.1 If the grievance has not been resolved to your satisfaction you may appeal in writing, stating your full grounds of appeal, within one week of the date on which the decision was sent or given to you. You will be informed to whom your appeal should be addressed.
- 17.4.2 We will hold an appeal meeting, normally within two weeks of receiving the appeal. Where possible, this will be dealt with impartially by a more senior manager who has not previously been involved in the case. You will have a right to bring a companion (see paragraph 17.3.2). We will confirm our final decision in writing, usually within one week of the appeal hearing. There is no further right of appeal.

SECTION 18

Anti-Slavery and Human-Trafficking Policy

18.1 POLICY STATEMENT

- 18.1.1 This policy applies to all persons working for us or on our behalf in any capacity, including employees at all levels, directors, officers, agency workers, seconded workers, volunteers, agents, contractors, and suppliers.
- 18.1.2 All companies in the SPS Group strictly prohibit the use of modern slavery and human trafficking in our operations and supply chain.
- 18.1.3 We have and will continue to be committed to implementing systems and controls aimed at ensuring that modern slavery is not taking place anywhere within our organisation or in any of our supply chains.
- 18.1.4 We expect that our suppliers will hold their own suppliers to the same high standards. Commitments Modern Slavery and Human Trafficking Modern slavery is a term used to encompass slavery, servitude, forced and compulsory labour, bonded and child labour and human trafficking.
- 18.1.5 Human trafficking is where a person arranges or facilitates the travel of another person with a view to that person being exploited. Modern slavery is a crime and a violation of fundamental human rights.

18.2 Commitments

- 18.2.1 We shall be a company that expects everyone working with us or on our behalf to support and uphold the following measures to safeguard against modern slavery:
- 18.2.2 We have a zero-tolerance approach to modern slavery in our organisation and our supply chains.
- 18.2.3 The prevention, detection and reporting of modern slavery in any part of our organisation or supply chain is the responsibility of all those working for us or on our behalf. Workers must not engage in, facilitate, or fail to report any activity that might lead to, or suggest, a breach of this policy.
- 18.2.4 We are committed to engaging with our stakeholders and suppliers to address the risk of modern slavery in our operations and supply chain.
- 18.2.5 We take a risk based approach to our contracting processes and keep them under review. We assess whether the circumstances warrant the inclusion of specific prohibitions against the use of modern slavery and trafficked labour in our contracts with third parties.
- 18.2.6 Using our risk based approach we will also assess the merits of writing to suppliers requiring them to comply with our Code of Conduct, which sets out the minimum standards required to combat modern slavery and trafficking.

SECTION 18

Anti-Slavery and Human-Trafficking Policy

18.2.7 Consistent with our risk based approach we may require:

- Employment and recruitment agencies and other third parties supplying workers to our organisation to confirm their compliance with our Code of Conduct
- Suppliers engaging workers through a third party to obtain that third parties' agreement to adhere to the Code.

18.3 As part of our ongoing risk assessment and due diligence processes, we will consider whether circumstances warrant us carrying out audits of suppliers for their compliance with our Code of Conduct.

18.4 If we find that, other individuals or organisations working on our behalf have breached this policy we will ensure that we take appropriate action. This may range from considering the possibility of breaches being remediated and whether that might represent the best outcome for those individuals impacted by the breach to terminating such relationships.

SECTION 19

SPS Group Sickness Absence Management Procedure

SPS Group Services
(Incorporating SPS Security Ltd., SPS Technical Services, Independent Cleaning Services Ltd.)

19.1 INTRODUCTION

Good attendance by all employees is essential to the effective and efficient operation of the Company and its contracts. Sickness absence management is fundamental in the planning and provision of a quality service and to maintaining high morale amongst all employees.
Attached are Guidance documents, which must be read in conjunction with the application of the procedure. These notes provide further clarity on the context in which the procedure has been developed.

19.2 SCOPE

This procedure applies to all employees of the SPS Group,

The Sickness Absence Management procedure has been developed to provide a fair, consistent, and supportive framework for the effective management of sickness absence. It also provides a structured procedure for dealing with cases where an employee’s sickness absence is cause for serious concern.

19.3 STATEMENT

Employers have a duty of care to all employees and to expect employees to attend work on a regular basis. This procedure aims to provide a framework to achieve good attendance through supportive, firm, fair and consistent management. The procedure is designed to balance the needs of the company requirements with the needs of the employees who are ill and those employees who remain at work.

19.4 PRINCIPLES

The principles behind the development of the procedure are to develop a working environment and management style that:

- Values and encourages good attendance. • Supports and respects the dignity of employees who are ill
- Recognises and respects confidentiality in dealing with medical information and sickness absence.
- Treats employees in a fair, sensitive, and consistent manner, recognising the individual circumstances.
- Maintains accurate sickness absence records to identify absence issues at an early stage using this information and other appropriate information (e.g. medical reports) to objectively manage sickness absence.

SECTION 19

SPS Group Sickness Absence Management Procedure

- Is collaborative and open in approach with employees who are absent through sickness, ensuring early, regular contact and consultation about possible solutions to sickness absence.
- Ensures that appropriate medical advice is sought, when necessary, and acted upon.
- Distinguishes between sickness incapacity and issues of conduct, addressing each separately on its own merit, through the appropriate procedure.

19.5 ROLES AND RESPONSIBILITIES

- 19.5.1** Senior Operations Manager / Commercial Director
- (i)** To ensure that the Procedure (including the Sickness Notification Procedure) is communicated to all staff and implemented.
 - (ii)** To hear cases and any appeals arising from the implementation of the Procedure
 - (iii)** To ensure that the appropriate and suitably trained senior member of staff carries out his/ her responsibilities in accordance with the Procedure.

19.5.2 The Group Projects & Compliance Manager

The day-to-day management of sickness absence is the responsibility of the Group Projects & Compliance Manager.

The Group Project & Compliance Manager may delegate responsibility for dealing with the initial stages of the procedure to appropriate senior designated and suitably trained member(s) of staff.

The Group Project & Compliance Manager has a crucial role in the successful management of sickness absence and a number of specific responsibilities.

- These are:
1. To know and understand the levels of attendance amongst employees. To ensure that sickness absence levels are recorded, monitored and information kept on the duration, frequency, and reasons for sickness absence.
 2. To treat employees fairly and consistently in applying the Procedure, to adopt a consistent approach, which is seen to be fair to all employees. To take into account the individual’s circumstances when reviewing sickness absence and deciding on what action to take.

SECTION 19

SPS Group Sickness Absence Management Procedure

- 3. To take an interest in the health of employees and encourage good attendance and where health problems are identified to put in place support mechanisms that allow and encourage good attendance.
- 4. To involve representatives in the process. The support and involvement of representatives is an important component of managing sickness absence. The Group Project & Compliance Manager must give the opportunity for them to be involved at the appropriate stage of the procedure. This will reassure employees and increase their trust and confidence in the process.

19.5.3 THE EMPLOYEE

- 1. To attend work when fit to do so.
- 2. To comply with the Procedure, the Sickness Notification Procedure and to submit medical certificates to the company at the appropriate times.
- 3. To keep the account Manager and the company informed of the situation when absent from work including progress or changes in his/ her medical condition.
- 4. To attend meetings with the Account Manager, or The Group Project & Compliance Manager as required and to discuss sickness and health issues, as is reasonable and appropriate.

19.5.4 THE SPS CONTROL ROOM / ICS ADMIN

- 1. To comply with the control room / ICS Admin Procedure in relation to inputting into time gate all employee Absence and sicknesses notified to them.

19.6 SICKNESS NOTIFICATION AND REPORTING PROCEDURE

19.6.1 SICKNESS NOTIFICATION

The Company shall adopt a clear Sickness Notification Procedure, which has been communicated to each member of staff. All new employees, as part of their induction, will receive a copy of the Sickness Notification Procedure.

Failure to comply with the Sickness Absence Reporting Procedure may affect pay and can lead to disciplinary action.

SECTION 19

SPS Group Sickness Absence Management Procedure

19.6.2 SICKNESS RECORDING

To ensure effective sickness absence management there is a need to monitor and review the levels and reasons for absence in a regular, sustained, and consistent way. The Company will accurately record and monitor sickness absence. For Sick Pay purposes, sickness absence is reported in full days. In situations where an employee arrives for work but is unwell and unable to remain at work, this absence still needs to be reported. However, absences of this nature will continue to be recorded and monitored for absence management purposes against y trigger points.

19.7 RETURN TO WORK PROCEDURE

Return to work contact & assessment should be made with each employee after every period of sickness absence. [See Appendix 19.9.7, page 77, Return to Work Questionnaire]. a suitably trained senior member of staff [Site Manager/Supervisor] must do this as soon as possible on the first day of return to:

- Confirm the reason for the absence (for recording purposes)
- Ensure that the employee feels fit and well enough to return.
- Update the employee on any work-related issues.
- Discuss any advice offered on the employees ‘Fit Note’ or support that may be needed.

This provides an informal opportunity to discuss the absence and any issues arising, to explore if there are any underlying causes and to identify any areas where support may be needed. The return-to-work interview form should be completed during this meeting including identifying exactly why the employee had been absent.

These discussions do not constitute the formal part of the procedure but are part of the basic supervisory relationship. Following an employee returning to work after a prolonged absence it may be beneficial to have regular sickness review meetings which are not “formal action”. These meetings would give the opportunity to keep the employee’s health management under review.

19.8 SICKNESS REPORTING PROCEDURE

1st Day of Absence

If you are unable to attend work due to sickness that you must make verbal contact by telephone with the SPS Control Room / ICS Area Manager.

SECTION 19

SPS Group Sickness Absence Management Procedure

The employee must give the nature (that is a description of the symptoms that mean they are unable to attend work because of their sickness) and anticipated duration of their absence.

Use of text and email is not acceptable. If no communication is received by you then we ask that a family member makes, contact.

Daily

If you continue to be absent, please keep daily contact with the Control Room / Area Manager

by 5th Day

The employee must submit to the company a Self-Sickness Certificate for any period of absence up to and including 7 days. [Sickness on Saturdays, Sundays and Bank Holidays must be included as part of the period of sickness].

8th Day

If the period of sickness continues beyond 7 calendar days, the employee must present a GP’s medical certificate covering the period of absence after the Self Certificate.
Failure to provide certificates may result in a loss of pay.

Medical Certificates

Medical Certificates must be presented to the company on immediate receipt from your GP this will assist the company to provide sick pay.

Failure to provide a Medical Certificate is a breach of the Company Sickness & Absence procedure and may prohibit sickness payments being made to you.

You may be asked to post Self Signed Certificates & Medical Certificates to the SPS Pay Office.

Absence Longer Than 8 Days

When more than one period of sickness of seven days or less occurs within a 28 day period, the company also requires a GP’s medical certificate. Any employee who has exceed 20 consecutive days of absence or

SECTION 19

SPS Group Sickness Absence Management Procedure

has had more than 4 separate occurrences of absence within a 12 month period will be dealt with under the monitoring procedure.

19.9 MANAGEMENT OF SHORT-TERM SICKNESS

19.9.1 INTRODUCTION

This section should be used where employees have high levels of short-term sickness absence, either caused by related or unrelated medical condition(s) and is intended to facilitate discussions between the manager and employee to understand the basis for the absence; identify what support is required; clarify expectations and ultimately determine whether the individual is incapable of performing their role on health grounds.

19.9.2 Attendance Score

The College uses an increasingly common absence-management initiative which helps to identify individuals with poor sickness absence records, referred to as the Bradford Factor or Bradford Formula. It produces points score for each person, based on their absence records but weighted so it gives more prominence to frequent short periods of absence. It is calculated in this way:

$$A \times A \times D$$

Where A is the number of absences (then the number is multiplied by itself) and D is the total number of days’ absence taken. The calculation is based on a rolling 52-week period.

19.9.3 Trigger Points

Attendance Scores will be calculated by The Group Project & Compliance Manager for all employees and sent out to managers on a regular basis. Managers must monitor the scores for their teams and take the appropriate action when the Score reaches a certain level or “trigger” point.

Where an employee’s absence reaches one or more of the following trigger points, the manager will take action following the procedure set out below:

- 51 points – Informal Absence Review Meeting.
- 101 points – Stage 1: Formal Absence Review Meeting – Verbal warning

SECTION 19

SPS Group Sickness Absence Management Procedure

- 201 points – Stage 2: Formal Absence Review Meeting – Written warning
- 401 points – Stage 3: Formal Absence Review Meeting – Final warning
- 601 points – Formal Absence Review Meeting – Dismissal

Whenever these triggers are reached within the year then action should be taken, so if a score of 51 or more is reached within the first 3 months, then action should be taken at that trigger point. NB Absence from work due to illness directly related to a disability, or where a person classed as disabled requires leave which is directly associated with their disability, will need to be accommodated within the terms of the Act and should not be included in the scoring process. General sickness absence – which will apply to disabled and non-disabled people – is unaffected by the Act and the arrangements detailed above will apply.

If the absence trigger is reached due to one period of pre-planned absence (e.g. for planned surgery) then it may be inappropriate to progress this matter further. Seek Human Resources advice if unsure.

At all stages of this process, a written record of all meetings and actions should be kept on the employee's secure departmental file. These records should be signed by both the manager and employee and made available to the Human Resources Department on request.

19.9.4 THE PROCESS

Informal Absence Review Meeting (Attendance Score Trigger = 51 points)

The manager should meet with the employee to discuss their sickness absence and the reasons for this. Where the manager is concerned that there may be an underlying cause for the absences and feels that further information would assist their management of the situation; they may use their judgement and refer the employee to Occupational Health.

The required improvement in attendance and the consequences of no or little improvement should be clearly explained.

SMART (Specific, Measurable, Achievable, Realistic and Time limited) objectives should be agreed with

SECTION 19

SPS Group Sickness Absence Management Procedure

a review date set (usually a 3-month review period) and confirmed in writing to the employee. The Attendance Management Action Plan (Appendix 19.9.3) should be used to support this process.

During the agreed period (up to 3 months) the manager will meet with the employee after each episode of sickness should it occur or on a monthly basis if agreed to review the objectives determined at the initial Informal Absence Review Meeting. If there has been an improvement and objectives have been met at the end of the agreed period, then the process can be signed off by both parties and discontinued.

Should the level of sickness absence continue to warrant concern and/or the objectives have not been met, then the manager should progress to the formal stage of the procedure. If an employee has breached their objectives by the time of any of the review meetings, then there is no need to wait for the 3-month period to expire before progressing to the formal stage.

Once the trigger for the Informal Absence Review has been reached then an employee would be expected to have no more than one episode of more than 4 days. Two absences in a 3-month period therefore would automatically place staff on the next stage.

Formal Absence Review Meeting

If, following the Informal Absence Review Meeting the employee has not been able to improve their attendance, the employee will be required to attend a Formal Absence Review Meeting.

At all formal stages of the process, it is recommended that the manager is supported by The Group Project & Compliance Manager, and it is the legal right of the employee to be accompanied by either a trade union representative or work colleague.

At each meeting the manager should be fully prepared with the issues they wish to address and have accurate evidence of the employee's sickness history to hand to support any concerns to be addressed.

The manager will write to the employee inviting them to the Formal Absence Review Meeting and outlining the purpose of the meeting, informing them of their right to be accompanied by their trade union representative or a work colleague. The employee must be asked if they require any reasonable adjustment in order that they attend the meeting, such as timing, accessibility of venue.

SECTION 19

SPS Group Sickness Absence Management Procedure

The manager will explain to the employee that their absences have reached a level that is considered unsatisfactory and the reasons why this is the case.

The employee will be given a full and fair opportunity to explain the absences and put forward any mitigating factors or other representations.

After hearing the employee, a manager should issue a formal warning in line with the trigger point guidance above. Issuing a formal warning does not mean that managers doubt whether any sickness absence was genuine. The caution is issued due to the unacceptable level of sickness absence.

The required increase in attendance, and the consequences of no or little improvement, should be clearly explained.

SMART (Specific, Measurable, Achievable, Realistic and Time limited) objectives should be agreed with a review date set (maximum 3-month review period) and confirmed in writing to the employee. The Attendance Management Action Plan
The formal warning will remain “live” on the employee’s file for the 12-month period.

Formal Warning:

Stage 1 – Verbal Warning (Attendance Score Trigger = 101 points)

Stage 2 – Written Warning (Attendance Score Trigger = 201 points)

Stage 3 – Final Warning (Attendance Score Trigger = 401 points)

A formal warning should:

- State the problem from the employer’s perspective, i.e. that attendance has been unsatisfactory and that this has caused problems in terms of getting the employee’s work done reliably and efficiently;
- Quote the precise number of absences and the total number of days of absence over a defined period of time.
- State that it is a written warning that forms part of the Company formal procedure.
- Set out the required improvement in attendance and the timescale in which the employee should strive to achieve this;

SECTION 19

SPS Group Sickness Absence Management Procedure

- State when the matter will be reviewed again.
- State how long the warning will remain ‘live’ in the employee’s file.
- Make clear that if the employee’s level of attendance does not improve to the required standard within the given time period, further formal action will be taken.
- State that the employee may appeal against the warning, and to whom any such appeal should be directed.

It is appropriate to issue a warning even in circumstances where the employee’s absences have all been for genuine reasons of ill health. The warning will be on the grounds of unsatisfactory attendance, and not on account of ill health, a distinction that should be made plain.

In this way it is clear that the employee is not being blamed for the absences but is nevertheless put on notice that their attendance is unsatisfactory from the point of view of the Company as employer.

Dismissal (Attendance Score Trigger = 601 points)

Where an employee is on their final written warning, and there is still no significant improvement in attendance, a senior post holder (the dismissing manager) may take the decision to dismiss the employee on the grounds of unacceptable level of attendance.

The “dismissing manager” should write to the employee setting out their concerns and invite them to attend a meeting making clear that the outcome could be dismissal. Again, the employee has the right to be accompanied by a trade union representative or work colleague. The manager presenting the evidence will also be in attendance.

Any decision to dismiss should be made following a final meeting with the employee and their representative once all other alternatives have been exhausted.

If an employee fails to attend any of the above meetings (without prior and reasonable explanation) then the manager will make a decision based on the information available at that time.

SECTION 19

SPS Group Sickness Absence Management Procedure

19.9.5 Right of Appeal

Appeals against Verbal, First and Final Written Warnings.

Appeals will normally be dealt with by the next higher level of line management to that level of management imposing the warning. Appeals must be made in writing to the ‘senior manager’ within 5 working days of the date of the warning and must state the grounds for appeal.

Appeal against Dismissal

An employee who is dismissed should be given written notice in accordance with the statutory minimum, or their contractual notice period, whichever is the greater. An employee can appeal against their dismissal, in writing, within 10 days of receipt of the decision to dismiss.

After the appeal hearing has been held the ‘senior manager’ will notify the employee of their decision, in writing. The manager’s decision is final.

SECTION 19

SPS Group Sickness Absence Management Procedure

19.9.6 RETURN TO WORK QUESTIONNAIRE

Name of Employee:		Clock No:
Period of Sickness	From:	To:
Number of Days Sickness in last 12 months:		Number of Periods:
Number of Days Absence in last 12 months:		Number of Periods:
What was the reason for your period of sickness/absence?		
Why did this restrict you from coming to work?		
What aspects of work could you not do and why?		

SECTION 19

SPS Group Sickness Absence Management Procedure

Did you visit your doctor or the Hospital? YES/NO
If yes, give details:
Have you got to see the doctor again? YES/NO
When/Why?
Did you receive any medication from either the Doctor or Hospital? YES/NO
If yes, give details:
How long have you got to take this for?

SECTION 19

SPS Group Sickness Absence Management Procedure

Are there any side effects that might affect you and your ability to carry out your duties e.g., must not operate machinery? YES/NO
If yes, give details:
Is this a recurrence of a previous illness? YES/NO
If yes, give details:
Do you believe the illness is likely to recur? YES/NO
If yes, give details:
Is there anything the company can do to avoid this happening e.g. different chair for a poor back?

SECTION 19

SPS Group Sickness Absence Management Procedure

Are you aware that, over the last 12 months, you have taken days/ periods of leave through sickness/absence?	
Employee’s comments:	
Interviewer’s comments:	
I understand that if I provide inaccurate or false information about my absence from work, it may, depending on the circumstances, be treated as Gross Misconduct which may lead to my being Summarily Dismissed from the Company.	
Employee’s Signature:	Date:
Interviewer’s Name:	Signature:

SECTION 19

SPS Group Sickness Absence Management Procedure

Additional information (may include more details from the individual, a copy of sickness record)
Action to be taken (if any, maybe investigation into the allergic reaction – what other substances are available?)

SECTION 20

SPS Group Services Customer Care Policy

SPS Group Services

(Incorporating SPS Security Ltd, SPS Technical Services, Independent Cleaning Services Ltd)

Customer Care Policy Statement & Standards

Whenever customers have contact with the SPS Group Services they will receive consistently high standards of customer service. These standards will ensure that all sections of the community are able to access our services. We are committed to ensuring that customer service excellence is an integral part of the planning, resourcing, and delivery of all our services.

Policy Statement

As an organisation SPS Group Services will be:

- Helpful and courteous in delivering high quality services.
- Professional and positive in our approach, taking pride in what we do.
- Well informed, so that our customers know what they can expect from us.
- Effective in listening to customers when they express dissatisfaction or complain.
- Fair and equitable towards individuals and communities with differing needs.

Who are our customers?

Our customers are all the people we come into contact within, connection with our work. This includes any contractors, visitors or staff that operate, visit or work on any contract.

What do our customers want?

Our customers want accessible, efficient, consistent, and responsive services and information, and we must strive to meet these demands.

What is customer care and why is it so important?

Because poor customer care is expensive – it loses customers, potential and existing clients and hard-fought reputations.

SECTION 20

SPS Group Services Customer Care Policy

Customer care means:

- Providing a good quality service and efficient service in a helpful way.
- Treating other people how they would like to be treated.
- Treating each person as an individual.
- Treating people with dignity, respect, and courtesy.
- Offering choices where possible.
- Clearly explaining when there are no choices.

In order to do this, we must understand and recognise that all our customers are different and that they all have diverse needs. These differences and needs can be based on culture, language, ethnicity, age, gender, disability, literacy, sexual orientation, or religion.

Good customer care is about having a positive attitude towards, and respect for, diversity and in turn, having the flexibility to adapt our behaviour and actions in a way that is appropriate for the individual.

Why do we need customer care standards?

Apart from the common-sense business approach stated above there are other good reasons for adopting customer care standards.

Customer care standards set out the expectations on our employees in their work and ensure that we become and remain a customer-focussed organisation. In particular, these standards define a corporate customer care framework for the achievement of excellent customer service which ensures that all customers, whether they are staff, contractors, or visitors, receive the same consistent, high standards of customer service.

How do we maintain our Customer Care Policy?

The development of our Customer Care Policy is an important part of our Human Resource Strategy, which aims to ensure that our workforce can organise and deliver quality services. This is delivered by:

- Focusing on service priorities
- Reshaping our organisation on a regular basis
- Developing our skills and performance
- Improving internal and external communication

Specific training will be provided to staff to help them carry out the Customer Care Policy. The policy will be maintained by all staff and managers, each manager will have no more than 12 customers to which they will be responsible.

SECTION 20

SPS Group Services Customer Care Policy

How will we measure our success?

We will monitor our performance through self-assessment and through receiving feedback from internal and external inspections. The SPS Customer Service Level Reviews are an excellent tool in this process.

Site Surveys will be held on a variety of sites to access our performance.

We must map and analyse any trends of complaint. These are discussed during every Operations and Senior Management meeting and acted on accordingly.

Every Manager will be expected to produce a Customer Service Level Review for every customer.

CUSTOMER CARE STANDARDS

General

- We will be polite and courteous.
- We will provide advice as and when appropriate on all our services.
- We will do our best to take ownership and provide any relevant information to visitors, contractors, and staff.
- We will keep records, analyse them and act upon the analysis.
- We will undertake work as we said we would, and in the time that we said we would, or will provide timely information to explain why this is not the case.
- We will keep customers informed at all stages of work.
- We will provide a safe environment for our customers.

Telephone Contact

- Our Head office will attempt to answer any incoming calls within five rings wherever possible and depending on work load at the time. This ruling will apply to any contract where our employees are responsible for answering the phone.
- We will greet callers politely and give our Company/Customer name.
- We will try to identify any special needs.
- We will thank the caller for their call.
- We will only use Voicemail in rare circumstances.

SECTION 20

SPS Group Services Customer Care Policy

- We will operate an Out of hours answer phone on the reception desk and a fully Operationally manned centre from our control centre which is 24/7.
- We will ensure that messages on voicemail and answer phones are clear and audible by testing them.
- We will respond to voicemail and other messages within 24 hours.

Written Contact (including emails)

- We will reply to all correspondence within the approved and agreed timeframe.
- We will provide a contact name, office address, email address and direct dial number in all correspondence.
- We will acknowledge complaints within one working day and complete the investigation with 10 days.
- We will write in plain English (as far as the technical aspects of our work allow)
- Where we require any assistance with translation, we shall seek an appropriate agency to provide this.

Face to Face Contact

- We will have fully qualified staff who are fully trained in accordance with current legislation on all our contracts.
- We will issue identity badges for all staff.
- We will have the Company name on all operational vehicles.
- We will keep all appointments made and will inform people well in advance if we have to cancel it, giving an alternative day/time and reason for cancellation.
- We will explain work to the customer as simply as possible and explain the next steps if further work is required.
- We will seek advice from customer when compiling our work Schedules & instructions.

In developing these standards, we sought to:

- Set standards which are user-friendly, customer-focused, and measurable.
- Clearly state how staff should behave in dealing with customers.
- Ensure that the customer’s safety is as high a priority as any other matter.
- Set performance targets which can be reviewed regularly.
- Give consideration to legislation, good practice, and national standards.
- Ensure staff are equipped to deliver services effectively and considerately.

SECTION 21

SPS Group Services Workplace Violence Policy

SPS Group Services
(Incorporating SPS Security Ltd, SPS Technical Services, Independent Cleaning Services Ltd)

The SPS Group maintains a zero tolerance standard of violence in the workplace. The purpose of this policy is to provide our employees guidance that will maintain an environment at and within (SPS Group Services and Customer) property and events that is free of violence and the threat of violence.

POLICY:
Violent behavior of any kind or threats of violence, either implied or direct, are prohibited within the SPS Group and on any contract which we provide our services to. Such conduct by an SPS Group employee will not be tolerated. Any employee who exhibits violent behavior may be subject to criminal prosecution and shall be subject to disciplinary action up to and including dismissal. Violent threats or actions by a non-employee may result in criminal prosecution. The SPS Group will investigate all complaints filed and will also investigate any possible violation of this policy of which we are made aware. Retaliation against a person who makes a complaint regarding violent behavior or threats of violence made to him/her is also prohibited.

DEFINITIONS:
Workplace Violence: Behavior in which an employee, former employee or visitor to a workplace inflicts or threatens to inflict damage to property, serious harm, injury or death to others at the workplace.

Threat: The implication or expression of intent to inflict physical harm or actions that a reasonable person would interpret as a threat to physical safety or property.

Intimidation: Making others afraid or fearful through threatening behavior.

Zero-tolerance: A standard that establishes that any behavior, implied or actual, that violates the policy will not be tolerated.

Court Order: An order by a Court that specifies and/or restricts the behavior of an individual. Court Orders may be issued in matters involving domestic violence, stalking or harassment, among other types of protective orders, including Temporary Restraining Orders.

SECTION 21

SPS Group Services Workplace Violence Policy

PROHIBITED BEHAVIOR:
Violence in the workplace may include but is not limited to the following list of prohibited behaviors directed at or by a co-worker, supervisor, or member of the public:

1. Direct threats or physical intimidation.
2. Implications or suggestions of violence.
3. Stalking.
4. Possession of weapons of any kind on any SPS Group Services Contract or property, other exterior premises or while engaged in activities for SPS in other locations.
5. Assault of any form.
6. Physical restraint, confinement.
7. Dangerous or threatening horseplay.
8. Loud, disruptive, or angry behavior or language that is clearly not part of the typical work environment.
9. Blatant or intentional disregard for the safety or well-being of others.
10. Commission of a violent felony or misdemeanor on any SPS contract or within the Head Office
11. Any other act that a reasonable person would perceive as constituting a threat of violence.

Domestic Violence, while often originating in the home, can significantly impact workplace safety and the productivity of victims as well as co-workers. For the purposes of this document, “domestic violence” is defined as abuse committed against an adult or fully emancipated minor. Abuse is the intentional reckless attempt to cause bodily injury, sexual assault, threatening behavior, harassment, or stalking, or making annoying phone calls to a person who is in any of the following relationships:

- Spouse or former spouse;
- Domestic partner or former domestic partner;
- Cohabitant or former cohabitant and or other household members;
- A person with whom the victim is having, or has had, a dating or engagement relationship;
- A person with whom the victim has a child.
- SPS recognises that domestic violence may occur in relationships regardless of the marital status, age, race, or sexual orientation of the parties.

SECTION 21

SPS Group Services Workplace Violence Policy

REPORTING ACTS OR THREATS OF VIOLENCE:

An employee who:

- 1. Is the victim of violence, or
- 2. Believes they have been threatened with violence, or
- 3. Witnesses an act or threat of violence towards anyone else shall take the following steps:
 - If an emergency exists and the situation is one of immediate danger, the employee shall contact the local police by dialing 999 and may take whatever emergency steps are available and appropriate to protect himself/herself from immediate harm, such as leaving the area. He/She should contact our Control Centre for further advice.
 - If the situation is not one of immediate danger, the employee shall report the incident to the appropriate supervisor or manager as soon as possible and complete the Incident Report Form.

PROCEDURES- FUTURE VIOLENCE:

Employees who have reason to believe they, or others, may be victimized by a violent act sometime in the future, at the workplace or as a direct result of their employment with SPS, shall inform their supervisor by immediately completing a Workplace Violence Incident Report Form so appropriate action may be taken. The supervisor shall inform his/her Director/Manager and if necessary, will report it to the customer.

INCIDENT INVESTIGATION:

Acts of violence or threats will be investigated immediately in order to protect employees from danger, unnecessary anxiety concerning their welfare, and the loss of productivity. Procedures for investigating incidents of workplace violence include:

- Visiting the scene of an incident as soon as possible.
- Interviewing injured and threatened employees and witnesses.
- Examining the workplace for security risk factors associated with the incident, including any reports of inappropriate behavior by the perpetrator.
- Determining the cause of the incident.
- Taking mitigating action to prevent the incident from recurring. – Recording the findings and mitigating actions taken.

SECTION 21

SPS Group Services Workplace Violence Policy

MITIGATING MEASURES:

Incidents which threaten the security of employees shall be mitigated as soon as possible following their discovery. Mitigating actions include:

- Notification to the Police and relevant authorities when a potential criminal act has occurred.
- Provision of emergency medical care in the event of any violent act upon an employee.
- Post-event, trauma counseling for those employees desiring such assistance.
- Assurance that incidents are handled in accordance with the Workplace Violence Prevention policy.

TRAINING AND INSTRUCTION: SPS Group Services will ensure that all employees, including managers and supervisors, are provided training and instruction on general workplace security practices. The Group Managing Director shall be responsible for ensuring that all employees, including managers and supervisors, are provided training and instructions on job specific workplace security practices.

Training and instruction shall be provided as follows:

- To all current employees when the policy is first implemented.
- To all newly hired employees, supervisors and managers, or employees given new job assignments for which specific workplace security training for that job assignment has not previously been provided.
- To affected employees whenever management is made aware of a new or previously unrecognized hazard.
- Workplace security training and instruction includes, but is not limited to, the following:
 - Preventive measures to reduce the threat of workplace violence, including procedures for reporting workplace security hazards.
 - Methods to diffuse hostile or threatening situations.
 - Escape routes.
- Explanation of this Workplace Violence Prevention Policy.

In addition, specific instructions shall be provided to all employees regarding workplace security hazards unique to their job assignment.



01482 226 570

spsgroupservices.com

Neptune House, Neptune Street, Hull HU3 2BP