PRIVACY AND PERSONAL DATA PROTECTION POLICY

1. Introduction

1.1 We are strongly committed to protecting personal data. This policy describes how we collect and use personal data and provides information about individuals' rights. It applies to personal data provided to us, both by individuals themselves or by others.

1.2 Personal data is any information relating to an identified or identifiable living person. When "you" or "your" are used in this statement, we are referring to the relevant individual who is the subject of the personal data.

1.3 We currently use CCTV and other surveillance systems to help maintain a safe and secure environment for all staff, visitors and customers. Our Surveillance Systems Code of Practice is set out in the Appendix to this policy and describes how we use and protect any personal data that we collect as a result of our use of CCTV and other surveillance systems.

2. Principles of data protection

2.1 We will comply at all times with the following key principles of data protection when dealing with your personal data:

a) Lawful, fair and transparent - Data collection must be fair, for a legal purpose, and open and transparent as to how the data will be used.

b) Limited for its purpose - Data must only be collected for a specific purpose.

c) Data minimisation - Any data collected must be necessary and not excessive for its purpose.

d) Accurate - The data we hold must be accurate and kept up to date.

e) Retention - We must not store data longer than necessary.

f) Integrity and confidentiality - The data we hold must be kept safe and secure.

3. Special categories of personal data

3.1 Certain special categories of data are deemed to create more significant risks to a person's fundamental rights and freedoms (for example by putting you at risk of unlawful discrimination). Such special categories may include information about an individual's race; ethnic origin; politics; religion; trade union membership; genetics; biometrics (where used for ID purposes); criminal convictions; health and sexual orientation.

3.2 The processing of special categories of personal data about you requires your *explicit* consent, save in exceptional circumstances or where we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

4. Accuracy and relevance

We will take steps to ensure that any personal data that we process about you is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless you have agreed to this or would otherwise reasonably expect this.

5. Data Security

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

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

6. Data Retention

6.1 We will only retain your personal data 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.

6.2 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.

7. Transferring data internationally

Personal data may be transferred outside the European Economic Area (EEA), including to other members of our corporate group. Whenever we transfer personal data out of the EEA, we will take all steps reasonably necessary to ensure that any such transfer is made securely and there is adequate protection in place in order to protect such personal data.

8. Your Legal Rights

8.1 Under certain circumstances, you have rights under data protection laws in relation to your personal data. If you require further information on, or wish to exercise, any of the rights set out below, please contact us using the contact details set out below:

(a) Request access to your personal data (commonly known as a "data subject access request").
(b) Request correction of the personal data that we hold about you.
(c) Request erasure of your personal data.
(d) Object to processing of your personal data.
(e) Request restriction of processing of your personal data.
(f) Request the transfer of your personal data to you or to a third party.
(g) Withdraw consent at any time where we are relying on consent to process your personal data.

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

8.3 We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

8.4 We try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

9. Contact Details

9.1 If you have any questions about how we treat your personal data and protect your privacy, please write to our Data Protection Officer using the following contact details:-

Sembcorp Utilities (UK) Limited
Sembcorp UK Headquarters
Wilton International
Middlesbrough
TS90 8WS
For the attention of: Data Protection Officer
E: DPOUK@sembcorp.com
T:+44 (0)1642 212000

9.2 You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues (www.ico.org.uk).

Appendix

Surveillance Systems Code of Practice

Introduction

1.1 We believe that CCTV and other surveillance systems have a legitimate role to play in helping to maintain a safe and secure environment for all our staff, visitors and customers. However, we recognise that this may raise concerns about the effect on individuals and their privacy.

1.2 We are committed to complying with our legal obligations and ensuring the legal rights of staff, relating to their personal data, are recognised and respected. The following statement describes the type of data that we hold and how we use and protect such data.

1.3 References to **Surveillance Systems** in this document shall include fixed, adjustable and domed CCTV cameras designed to capture and record images of individuals and property, together with any other surveillance devices and/or systems designed to monitor or record images of individuals or information relating to individuals, including automatic number plate recognition (ANPR) and site access records.

2 Reasons for the use of Surveillance Systems

2.1 We currently use Surveillance Systems around the Wilton International Site as outlined below. We believe that the use of such use is necessary for legitimate business purposes, including (without limitation):-

a) to prevent crime and protect buildings and assets from theft, damage, disruption, vandalism and other crime;

b) for the personal safety of staff, visitors, customers and other members of the public and to act as a deterrent against crime;

c) to support law enforcement bodies in the prevention, detection and prosecution of crime;

d) to assist in the day-to-day management, including ensuring the health and safety of staff and others;

e) to monitor site access by individuals and/or vehicles; and

f) to assist in the defence of any civil litigation including employment tribunal proceedings and to assist in disciplinary and grievance matters.

3 Monitoring

3.1 The Surveillance Systems are in use 24 hours a day and data is continuously recorded.

3.2 Camera locations and viewing scopes are chosen to minimise the viewing of spaces not relevant to the legitimate purpose of the monitoring. Where cameras are adjustable, this will be restricted, in so far as is practical, to ensure operators cannot adjust them to overlook spaces not relevant to the legitimate purpose of the monitoring.

3.3 Appropriate signage is displayed at each of the gatehouse entrances to the Site to alert individuals that Surveillance Systems are in use and that their image may be recorded.

3.4 Live feeds from Surveillance Systems will only be monitored where this is reasonably necessary, for example, to protect health and safety.

3.5 We will ensure that live feeds from cameras and recorded images are only viewed by approved members of staff whose role requires them to have access to such data. This may include HR staff involved with disciplinary or grievance matters. Such staff will be given appropriate training to ensure they understand and observe the legal requirements related to the processing of relevant data.

4 Use of Data

4.1 In order to ensure that the rights of individuals recorded by the Surveillance Systems are protected, we will ensure that data gathered from Surveillance Systems is stored in a way that maintains its integrity and security.

4.2 Given the large amount of data generated by the Surveillance Systems, we may store video footage using a cloud computing system, We will take reasonable steps to ensure any cloud service provider maintains the security of our information.

4.3 We may engage data processors to process data on our behalf. We will ensure reasonable safeguards are in place to protect the security and integrity of the data.

5 Retention and Erasure

5.1 Data recorded by the Surveillance Systems will be stored digitally using a cloud computing system. Data from the Surveillance Systems will not be retained indefinitely and will be permanently deleted once there is no reason to retain the recorded information. Exactly how long images will be retained for will vary accordingly to the purpose of which they are being recorded. For example, where images are being recorded for crime prevention purposes, data will be kept long enough only for incidents to come to light.

5.2 At the end of their useful life, all images stored in whatever format will be erased permanently and securely. All physical matter such as tapes, discs and hard photographs will be disposed of as confidential waste.

6 Use of Additional Surveillance Systems

6.1 Prior to introducing any new Surveillance System (**New System**) we will carefully consider if they are appropriate by carrying out a privacy impact assessment (**PIA**).

6.2 A PIA is intended to assist us in deciding whether the New System is necessary and proportionate in the circumstances and whether they should be used at all or whether any limitations should be placed on their use.

6.3 Any PIA will consider the nature of the problem that we are seeking to address at that time and whether the New System is likely to be an effective solution, or whether a better solution exists. In particular, we will consider the effect the New System will have on individuals and therefore whether its use is a proportionate response to the problem identified.

6.4 No surveillance cameras will be placed in areas where there is an expectation of privacy (for example, in changing rooms) unless, in very exceptional circumstances, it is judged by us to be necessary to deal with very serious concerns.

7 Covert Monitoring

7.1 We will not engage in covert monitoring or surveillance (that is, where individuals are unaware that the monitoring or surveillance is taking place) unless, in highly exceptional circumstances, there are reasonable grounds to suspect that criminal activity or extremely serious malpractice is taking place and, after suitable consideration, we reasonably believe there is no less intrusive way to tackle the issue.

7.2 In the unlikely event that covert monitoring is considered to be justified, it will only be carried out with the express authorisation of the Site Director. The decision to carry out covert monitoring will be fully documented and will set out how the decision to use covert means was reached and by whom. The risk of intrusion on innocent workers will always be a primary consideration in reaching any such decision.

7.3 Only limited numbers of people will be involved in any covert monitoring. Such covert monitoring will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific suspected illegal or unauthorised activity.

8 Ongoing Review of Surveillance System Use

We will ensure that the ongoing use of Surveillance Systems in the workplace is reviewed periodically to ensure that their use remains necessary and appropriate, and that any Surveillance System is continuing to address the needs that justified its introduction.

9 Requests for Disclosure

9.1 We may share data with other group companies where we consider that this is reasonably necessary for any of the legitimate purposes set out above in paragraph 2.1.

9.2 No images from our Surveillance Systems will be disclosed to any other third party, without express permission being given by the Site Director. Data will not normally be released unless satisfactory evidence that it is required for legal proceedings or under a court order has been produced.

9.3 In other appropriate circumstances, we may allow law enforcement agencies to view or remove footage from our Surveillance Systems where this is required in the detection or prosecution of crime.