CHARLES & KEITH
GROUP

Code of Conduct for Employees

CHARLES & KEITH
GROUP

Contents

INTRODUCTION

CHARLES & KEITH Group (the "Group") is headquartered in Singapore and operates more than 600 stores worldwide under two brands specialising in fashion footwear and accessories – CHARLES & KEITH and PEDRO. Every day, our brands aim to shape fashion for the better through our group mission: Inspiring Fashion.

At CHARLES & KEITH Group, we believe that all employees should be able to work in an environment that reflects professionalism and integrity. With our Code of Conduct for Employees, we seek to establish transparent standards of conduct and duties for employees at work.

We want to ensure that all employees globally are provided with clear information regarding the range of policies and procedures when working in any of the CHARLES & KEITH Group companies. Some policies and procedures, such as the Diversity and Inclusion Policy, and the Harassment Policy are primarily designed to protect your rights while others, such as the Social Media Policy, and the Information Technology and Communications Policy lay down the standards which the Group expects all employees including former employees to follow at all times. The policies and procedures in this Code of Conduct for Employees (Full Version) are intended to provide employees with high-level guidelines which apply to employees at all times and in the event of any conflict with the terms of an employee's contract of employment and offer letter, the policies and procedures set out in this Code of Conduct for Employees (Full Version) shall prevail.

The Code of Conduct for Employees is regularly reviewed and updated to reflect any changes in relevant legislation as well as employees' needs, industry and best practices. An up-to-date copy of the Code of Conduct for Employees is available for all employees of the Group globally in the employee portal/company intranet.

If you have any questions about the contents of this Code of Conduct for Employees or other policies, please first contact your immediate supervisor, and then the Group's Talent Success Department.

1. GROUP CORE VALUES

The Group believes in shaping our culture by way of alignment on the core values of the Group. These core values and how they may be demonstrated are set out below:

1.1 Collaboration – Teamwork & Shared Goals

How do I demonstrate this value?

- I actively engage in teamwork to achieve shared goals and foster a culture of support and trust.
- I go the extra mile to help colleagues succeed, stepping in to assist when needed and celebrating our achievements together.
- By prioritising mutual respect and genuine connection, I contribute to a positive and productive work environment where everyone can thrive.

1.2 Creativity – Innovate and Inspire

How do I demonstrate this value?

- I dare to explore and break out of norms and inspire others to think out of the box.
- I am proactive in finding ways to improve work processes and other matters at the workplace.
- I anticipate and embrace changes to keep up with emerging business trends and adapt to digitalised processes that can achieve higher work efficiency.

1.3 Purpose-Driven – Impact beyond Profit

How do I demonstrate this value?

- I value cohesiveness in the Group regardless of brands, countries, business units and departments.
- I practise mindfulness by being sensitive and compassionate to the well-being and feelings of others.
- I come up with ideas and designs in line with the Group's sustainability goals and practise positive sustainable habits at the workplace.
- I seek opportunities to create meaningful change, whether through innovation, partnerships, or community involvement.

1.4 Empowerment – Thrive & Grow

How do I demonstrate this value?

- I take pride in expressing my unique individuality through fashion and work endeavours.
- I take ownership of my own development by cultivating self-awareness in areas of improvement and constantly seek opportunities to better myself through learning, and honing my knowledge and skills.
- I voice out and stand up for my ideas fearlessly, and ask for resources needed to achieve the department's goals.
- I share my thoughts and feelings considerately and remain open to feedback, debates and difficult conversations.
- I acknowledge my mistakes and shortcomings and embrace the lessons learned, and strive to do better moving forward.
- I recognise the strengths, attributes, and talents of our people and support them to actualise ideas and goals.
- I demonstrate characteristics of being dependable and accountable to build trust and confidence with our colleagues.

1.5 Respect & Openness – Inclusive and Transparent Culture

How do I demonstrate this value?

- I commit to cultivating a safe environment for our people to speak up by valuing everybody's differences as a collective power of teamwork and respecting everyone's ideas and voices.
- I promote transparency by being open about decisions, challenges I face, and the reasoning behind my actions.
- I embrace diversity by seeking out different perspectives and ensuring all voices are included and heard in discussions.

2. DIVERSITY AND INCLUSION POLICY

The Group recognises its talented and diverse workforce as a key long-term competitive advantage. We are committed to ensuring an inclusive environment for all employees regardless of their gender, race, ethnicity, national origin, age, sexual orientation or identity, education or disability. We are committed to a non-discriminatory approach by:

a. providing equal opportunity;

b. ensuring advancements in all of our departments, programmes, and worksites;

c. providing accommodations for disabilities (e.g., wheelchair ramps, handicap toilets, fire alarm lights for the hearing impaired, etc.); and

d. providing employee benefits for the wellbeing of our all our employees without prejudice basis.

The CHARLES & KEITH Group Diversity and Inclusion Policy is regularly reviewed and updated to ensure alignment with any changes the business model may undergo. Any grievances, questions or feedback may be directed to the Group's Talent Success Department.

3. HARASSMENT POLICY

3.1 Introduction

a. The Group recognises the right of all employees to be treated with respect and dignity and is committed to the development of positive policies for the elimination of all kinds of harassment and bullying. Harassment or bullying at work in any form is unacceptable and will not be permitted or condoned.

b. Harassment related to age, disability, gender, race and ethnicity, religion or belief, sex, or sexual orientation may be unlawful in your jurisdiction. Both the harasser and the Group may be held liable for this conduct. Harassment may be a criminal offence and may also give rise to a civil claim. It may also contravene health and safety legislations.

c. All Employees have the right to work in an environment free from harassment, bullying and any other form of intimidation. Only through fostering an inclusive and collaborative environment can we all thrive and maximise our employees' talent and potential.

d. This policy applies to all persons working for or representing the Group, which include without limitation directors, managers, agencies, workers, contractors, vendors, etc.

e. This Harassment Policy seeks to inform individuals of the types of behaviour that are unacceptable and provide employees who are the victims of harassment or bullying with a means of redress. The Group may amend the policy from time to time.

f. The Group will treat allegations of harassment or bullying seriously. Anyone found to be in breach of this policy will be liable to disciplinary action which could result in their dismissal.

3.2 What is Harassment?

a. Harassment takes many forms, occurs on a variety of different grounds and can be directed at one person or many people. Harassment is conduct indicating to the recipient that he or she is unwelcomed, singled out or ostracised and which the recipient finds offensive or unacceptable. This can be in the form of physical, verbal or non-verbal conduct. It can also include acts online, such as circulating information or images via e-mail, the internet or social messaging services. Acts can be considered harassment even if there was no intention to violate the recipient's dignity so long such acts had the same effect of doing so.

b. Conduct normally becomes harassment if it has persisted after it has been made clear that the recipient has regarded it as offensive, although a single incident may amount to harassment if it is sufficiently serious.

c. Harassment may involve conduct of a sexual nature (sexual harassment), or it may be related to age, disability, gender, marital or civil partner status, pregnancy or maternity, race, colour, nationality, ethnic or national origin, religion or belief, or sexual orientation. It may also include victimising someone because they have been willing to challenge harassment.

d. Harassment may include, without limitation, the following:

   i. unwanted physical conduct or "horseplay", including without limitation touching, pinching, pushing and grabbing;

   ii. continued suggestions for social activity after it has been made clear that such suggestions are unwelcome;

iii. sending or displaying material that is pornographic or that some people may otherwise find offensive (including emails, text messages, video clips and images sent by mobile phone or posted on the internet);

iv. unwelcome sexual advances or suggestive behaviour (even if the harasser may perceive the same as harmless);

v. racist, sexist, homophobic or ageist jokes, or derogatory or stereotypical remarks about a particular ethnic or religious group or gender;

vi. outing or threatening to out someone as lesbian, gay, bisexual or transsexual;

vii. offensive emails, text messages or social media content;

viii. mocking, mimicking or belittling a person's disability or physical appearance;

ix. ostracising, isolation or non-cooperation and exclusion; or

x. intrusion by pestering, spying and stalking.

e. 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.

3.3 What is Bullying?

a. Bullying is offensive, intimidating, malicious or insulting behaviour that can make a person feel vulnerable, upset, humiliated, undermined or threatened. It can take the form of physical, verbal and non-verbal conduct. Bullying may include, by way of example:

i. shouting at, being sarcastic towards, ridiculing or demeaning others;

ii. physical or psychological threats;

iii. overbearing and intimidating levels of supervision;

iv. inappropriate and/or derogatory remarks about someone's performance;

v. abuse of authority or power by those in positions of seniority; or

vi. deliberately excluding someone from meetings or communications without good reason.

b. 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.

3.4 Employees' Responsibilities

a. You have a responsibility to help ensure that the dignity of all employees is respected in the work environment. Everyone must comply with this policy and you must ensure that your behaviour to colleagues and third parties does not cause offence and could not in any way be regarded as harassment.

b. You must discourage harassment by making it clear that you find such behaviour unacceptable and by supporting colleagues who suffer such treatment and are considering making a complaint. You must alert your immediate supervisor or the Group's Talent Success Department in confidence to any incident of harassment to enable the Group to deal with the matter.

c. If you are a victim of harassment yourself, you may use the procedure described later in this policy.

d. Where you consider that you have been harassed or bullied by someone who is not an employee of the Group, you must report the harassment or bullying to your immediate supervisor or to the Group's Talent Success Department. The Group will then consider what action is appropriate to address that complaint and prevent any further incidents.

3.5 Managers' Responsibilities

a. Managers have a duty to implement this policy and to make every effort to ensure that harassment and bullying does not occur, particularly in work areas for which they are responsible.

b. Managers must:

i. explain this policy to their employees and ensure that every member of their team has access to it;

ii. be responsive and supportive to any employee who makes any allegation of harassment or bullying, provide clear advice on the procedure to be adopted and ensure that confidentiality is maintained;

iii. set a good example by treating all business partners, employees and customers with dignity and respect; and

iv. ensure that there is no victimisation or further instances of harassment or bullying once a complaint has been resolved.

3.6 The Group's Responsibilities

a. The Group will take steps to support the principles set out in this policy. It will:

i. ensure that adequate resources are made available to promote respect and dignity in the workplace and to deal effectively with complaints of harassment or bullying;

ii. communicate this policy to all employees and include information on this policy as part of its induction program; and

iii. ensure that managers and supervisors, and any other employees playing any part in operating the complaints procedure understand their responsibilities under this policy and will arrange appropriate training if this is required.

b. The Group's Talent Success Department will provide advice to those conducting any investigations under this policy and will be present in an advisory capacity at any hearings.

c. The Group's Talent Success Department will monitor and review the operation of this policy regularly.

3.7 Scope and Use of Harassment Procedure

a. Due to the seriousness with which the Group views harassment and bullying, informal and formal reporting procedures have been introduced.

b. If you are the victim of harassment or bullying, you must not hesitate to use this procedure for fear of victimisation. Retaliation against an employee who brings a complaint of harassment or bullying is a serious disciplinary offence which may constitute Gross Misconduct (see Annex A).

c. Given that it is easier to resolve harassment issues if they are reported at the earliest opportunity, you are strongly encouraged to report any instances of harassment or bullying if you think you have been harassed or bullied. By invoking the harassment procedure promptly, you help ensure that the issue is addressed in a timely manner, protecting your well-being and maintaining a respectful work environment.

3.8 Informal Procedure

a. If an incident happens which you think may be harassment or bullying, you may consider attempting to resolve the problem informally. In some cases, it may be sufficient to make it clear

to the harasser that their behaviour is unacceptable and that it must stop. If you are unable to do this face to face, a written request explaining the distress which the behaviour is causing, handed to the harasser, may be effective. Alternatively, if you feel such an action is too difficult or embarrassing, you may seek assistance from your immediate supervisor or a member of the senior management.

3.9 Formal Procedure

a. If the harassment or bullying continues, where serious harassment or bullying occurs or where you do not consider use of the informal procedure appropriate, you may consider bringing a formal complaint and then seek assistance from your immediate supervisor or a member of the senior management. If this course of action is not suitable, assistance may be sought from the Group Talent Success Department. All complaints will be considered seriously and dealt with promptly and in confidence.

b. You will have to put your complaint in writing and your immediate supervisor or the member of the senior management you approach will advise on who to address it to and what arrangements should be made to ensure that confidentiality is preserved. Your written complaint should, where possible, state:

   i. the name of the harasser or bully;

   ii. the nature of the harassment or bullying;

   iii. date(s) and time(s) when the incident(s) occurred;

   iv. names of witnesses (if any) to the incident; and

   v. the action (if any) already taken to stop it occurring.

c. As soon as a formal complaint of harassment has been received by the Group, the Group will determine whether action should be taken and, where possible, to separate you from the person against whom you have made the complaint.

d. A Director/Regional Head or a member of the senior management, will carry out a thorough investigation as quickly as possible, while maintaining confidentiality always (the “Investigator”). The Investigator shall, as far as possible, not relate to the allegation in any way. All employees interviewed during the investigation shall keep the matter confidential. Investigations will be handled with sensitivity and with due respect for both your rights and the rights of the person

against whom you have made the complaint. You will not be asked to provide details of the allegations repeatedly unless this is essential for the investigation.

e. The investigation will involve interviews with you and the person against whom you have made the complaint. Such person will be given full details of the nature of the complaint and will be given the opportunity to respond.

f. Both you and the person against whom you have made the complaint will have the rights to be each accompanied by another colleague at any interviews.

g. You will be informed in writing on the outcome of the investigation once it is completed.

   i. If your complaint is well founded, disciplinary action may be taken against the person whom you complained. Deliberate harassment, victimisation or serious bullying may result in summary dismissal. Where a lesser penalty is appropriate (e.g., a written warning), or where no formal disciplinary action is to be taken, this will be coupled with such action as the Group considers appropriate to help you continue working without embarrassment or anxiety. The Investigator may recommend the transfer of the harasser to a different work area or arrange for the amendment of working practices to minimise contact between you and the harasser.

   ii. If your complaint is not well founded, the Group will consider whether your own transfer should be arranged if this is your wish, subject to practical limitations.

h. Whether or not your complaint has been upheld, your immediate supervisor or the member of the senior management you approach will meet you on a regular basis, after your complaint has been resolved to ensure that there are no further issues that need to be addressed.

i. The Group takes these matters very seriously. However, malicious complaints of harassment or bullying can have a serious and detrimental effect upon a colleague. Any unwarranted allegation of harassment or bullying, made in bad faith, may be regarded as potential Gross Misconduct (see Annex A). This is to ensure that the integrity of this policy is upheld and maintained.

3.10 Appeals

a. If you are not satisfied with the outcome of the investigation, you may appeal against the outcome by requesting for the outcome to be reconsidered by another Director/Regional Head or member of the senior management. Such requests shall be made in writing within 5 working

days of the date you were informed of the outcome of the initial investigation, setting out as fully as possible the reasons why you wish to appeal. The Director/Regional Head or member of the senior management selected to hear your appeal will have had no previous involvement in your complaint, as far as possible ("Appeal Tribunal").

b. You will meet with the Appeal Tribunal to explain why you think the conclusion of the initial investigation was wrong. Thereafter, the Appeal Tribunal will determine whether any further investigations are required, and will carry out the same, if so. The decision of the Appeal Tribunal will be communicated to you and shall be final.

c. Employees who receive a warning or who are dismissed for harassment or bullying may appeal against the outcome.

3.11 Time Scales and Records

a. The Group will, as far as possible, conclude an investigation within 30 days of receipt of the formal complaint. Appeals will, as far as possible, be considered within 15 days of receipt of the written request. As the complexity of harassment and bullying complaints varies greatly, the Group may not always be able to meet these time limits. While it is always highly desirable to resolve all complaints at the earliest opportunity, this may not always be possible if the investigation is to be both thorough and fair.

b. Records will be made of all investigations and hearings, the outcome and the actions taken, and will be kept confidential.

c. The Group reserves the right to record meetings at any stage in the formal procedure. You are not permitted to make your own recording under any circumstances.

d. Questions regarding the Ethical Conduct or the Harassment Policy may be directed to the Group's Talent Success Department.

4. INFORMATION TECHNOLOGY AND COMMUNICATIONS SYSTEMS POLICY

4.1 Introduction

a. The Group's information technology and communications systems and all related software (collectively, "Information Systems"), are intended to promote effective communication and

working practices within the organisation. This policy outlines the standards you must observe when using these Information Systems, the circumstances in which the Group will monitor your use, and the actions the Group will take in respect of breaches of these standards.

b. This policy applies to all employees, officers, consultants, contractors, workers, volunteers, interns, casual workers, agency workers and anyone else who has access to our Information Systems wherever they are working and whether during working hours or not.

c. Misuse of Information Systems can damage the business and the Group's reputation. Breach of this policy may lead to disciplinary action and, in serious cases, may be treated as Gross Misconduct (see Annex A) leading to summary dismissal.

d. The Group may amend this policy at any time if it considers it appropriate to do so.

4.2 Responsibility for this Policy

a. The Management Committee has overall responsibility for the effective operation of this policy and for ensuring compliance with the relevant statutory framework. Day-to-day responsibility for operating the policy and ensuring its maintenance and review has been delegated to the Group's Head of Information Technology Department.

b. Managers have a specific responsibility to ensure the fair application of this policy and all employees are responsible for supporting colleagues and ensuring its success.

c. The Group's Information Technology Department will deal with requests for permission or assistance under any provisions of this policy and may specify certain standards of equipment or procedures to ensure security and compatibility.

4.3 Equipment Security and Passwords

a. You are responsible for the security of the equipment allocated to or used by you and must not allow it to be used by anyone other than in accordance with this policy.

b. You are responsible for the security of any computer terminal used by you. You must lock your terminal or log off when leaving it unattended or leaving the office, to prevent unauthorised users accessing the Information Systems in your absence. Anyone who is not authorised to access our network should only be allowed to use terminals under supervision.

c. Desktop personal computers and cabling for telephones or computer equipment must not be moved or tampered with without first consulting the Group's Information Technology Department.

d. You must use passwords on all information technology equipment, particularly items that you take out of the office. You must keep your passwords confidential and change them regularly. You must not use another person's username and password, or make available, or allow anyone else to log on using your username and password. On the termination of employment (for any reason) you must provide details of your passwords to your immediate supervisor or the Group's Information Technology Department and return any equipment, key fobs or cards.

e. If you have been issued with a laptop, tablet computer, smartphone or other mobile device, you must ensure that it is kept secure at all times, especially when travelling. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event of loss or theft. You should also be aware that when using equipment away from the workplace, documents may be read by third parties, for example, passengers on public transport.

4.4 Systems and Data Security

a. You must not delete, destroy or modify existing Information Systems, programmes, information or data (except as authorised in the proper performance of your duties).

b. You must not download or install software from external sources without the authorisation from the Group's Information Technology Department. This includes software programmes, instant messaging programmes, screensavers, photos, video clips and music files. Incoming files and data must always be virus-checked before they are downloaded. If in doubt, you may seek advice from the Group's Information Technology Department.

c. You must not attach any device or equipment to our Information Systems without authorisation from the Group's Information Technology Department. This includes any USB flash drive, tablet, smartphone or other similar device, whether connected via the USB port, Bluetooth connection or in any other way.

d. The Group monitors all emails passing through our Information Systems for viruses. You must exercise caution when opening unsolicited emails from unknown sources or an email which

appears suspicious, for example, if it contains a file whose name ends in .exe. Inform the Group's Information Technology Department immediately if you suspect your computer may have a virus. The Group reserves the right to delete or block access to emails or attachments in the interests of security. The Group also reserves the right not to transmit any email message.

e. You must not attempt to gain access to restricted areas of the network, or to any password-protected information, except as authorised in the proper performance of your duties.

f. You must be particularly vigilant if you use our information technology equipment outside the workplace and take such precautions as the Group may require from time to time against importing viruses or compromising the Information Systems' security. The Information Systems contains information which is confidential and subject to data protection legislation. Such information must be treated with extreme care and in accordance with our Data Protection Policy (Clause 5).

4.5 Email

a. Although email is a vital business tool, you must always consider if it is the appropriate method for a communication. Correspondence with third parties by email must be written professionally. Messages should be concise and directed only to relevant individuals. The Group's standard disclaimer must always be included.

b. You must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, or otherwise inappropriate emails. If you feel that you have been harassed or bullied or are offended by material received from a colleague via email, you should promptly inform your immediate supervisor or the Group's Talent Success Department.

c. You must take care with the content of email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Remember that you have no control over whether your email may be forwarded by the recipient. Avoid saying anything which would cause offence or embarrassment if it was forwarded to colleagues or third parties or found its way into the public domain.

d. Email messages may be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an email cannot be recovered for

the purposes of disclosure. All email messages should be treated as potentially retrievable, either from the main server or using specialist software.

e. You must not:
   i. send or forward private emails at work which you would not want a third party to read;
   ii. send or forward chain emails, junk emails, emails containing jokes or gossip;
   iii. contribute to Information Systems' congestion by sending trivial messages, copying or forwarding emails to those who do not have a real need to receive them, or using "reply all" unnecessarily on an email with a large distribution list;
   iv. sell or advertise using our Information Systems or broadcast messages about lost property, sponsorship or charitable appeals;
   v. agree to terms, enter into contractual commitments or make representations by email unless appropriate authority has been obtained;
   vi. download or email text, music and other content on the internet subject to copyright protection, unless the owner of such works explicitly allows this;
   vii. send messages from another person's email address (unless authorised) or under an assumed name; or
   viii. send confidential messages via email or the internet, or by other means of external communication which are or may not known to be secure.
f. If you receive an email in error, you must inform the sender.
g. Do not use your own personal email account to send or receive email for the purposes of our business. Only use the email account the Group has provided for you.
h. When in doubt, please check with your immediate supervisor or the Group's Information Technology Department.

4.6 Using the Internet

a. Internet access is provided primarily for business purposes. Occasional personal use may be permitted as set out below.
b. When a website is visited, devices such as cookies, tags or web beacons may be employed to enable the site owner to identify and monitor visitors. Such a marker could be a source of embarrassment to the visitor and us, especially if inappropriate material has been accessed,

downloaded, stored or forwarded from the website. Such actions may also, in certain circumstances, amount to a criminal offence if, for example, the material is pornographic in nature. This is further considered under the "Prohibited Use" section below (Clause 4.9).

c. You must not access any web page or download any image, document or other file from the internet which could be regarded as illegal, offensive, in bad taste or immoral. As a general rule, if any person (whether such person 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.

d. You must not under any circumstances use our Information Systems to participate in any internet chat room, post messages on any internet message board, or set up, or log text, or information on a blog or wiki, even in your personal time.

4.7 Personal Use of the Group's Information Systems

a. The Group permits the incidental use of its Information Systems to send personal email, browse the internet and make personal telephone calls subject to certain conditions set out below. Personal use is a privilege and not a right. It must not be overused or abused. The Group may withdraw permission for it at any time or restrict access at its sole discretion.

b. Personal use must meet the following conditions:

   i. use must be minimal and take place substantially out of normal working hours (i.e., during lunch hours, before or after official working hours);

   ii. personal emails should be labelled "personal" in the subject header;

   iii. use must not interfere with business or office commitments;

   iv. use must not commit us to any marginal costs; and

   v. use must comply with this policy and our other policies stated in this Code of Conduct for Employees.

c. You should be aware that personal use of our Information Systems may be monitored (see below) and, where breaches of this policy are found, disciplinary action may be taken. The Group reserves the right to restrict or prevent access to certain telephone numbers or internet sites if it considers personal use to be excessive.

4.8 Monitoring

a. The Group's Information Systems enable us to monitor telephone, email, voicemail, internet and other communications. For business reasons, and in order to carry out legal obligations as an employer, use of the Information Systems including telephone and computer systems, and any personal use of them, may be continually monitored by automated software or otherwise. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.

b. Where applicable, a closed-circuit television ("CCTV") system monitors the work premises 24 hours a day. This data is recorded and may be referred to, in the event of any disputes/disagreements arising in the workplace.

c. The Group reserves the right to retrieve the contents of email messages or check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the business, including but not limited to the following purposes:

   i. to monitor whether the use of the email system or the internet is legitimate and in accordance with this policy;

   ii. to find lost messages or to retrieve messages lost due to computer failure;

   iii. to assist in the investigation of alleged wrongdoing; or

   iv. to comply with any legal obligation.

4.9 Prohibited Use of the Group's Information Systems

a. Misuse or excessive personal use of our Information Systems or inappropriate internet use will be dealt with in accordance as Gross Misconduct (Annex A). Misuse of the internet may in some circumstances be a criminal offence. It may amount to Gross Misconduct (see Annex A), to misuse our Information Systems by participating in online gambling, forwarding chain letters, or by creating, viewing, accessing, transmitting or downloading any of the following material (this list is not exhaustive):

   i. pornographic material (i.e., writing, pictures, films and video clips of a sexually explicit or arousing nature);

   ii. offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or to our clients;

iii. a false and defamatory statement about any person or organisation;

iv. material, which is discriminatory, offensive, derogatory or may cause embarrassment to others;

v. confidential information about the Group or any of the Group's employees or clients (except as authorised in the proper performance of your duties);

vi. any other statement which is likely to create any criminal or civil liability (for you or the Group); or

vii. music or video files or other material in breach of copyright.

b. Any such action will be treated very seriously and may result in summary dismissal.

c. Where evidence of misuse is found, the Group may undertake a more detailed investigation, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved. If necessary, such information may be handed to the police in connection with a criminal investigation.

d. Questions regarding Information Technology and Communications Systems Policy may be directed to the Group's Information Technology Department.

5. SOCIAL MEDIA POLICY

5.1 Purpose and Scope

a. This policy covers all forms of social media, including Facebook, LinkedIn, Twitter, YouTube, Wikipedia, WhatsApp, Skype, other social networking sites, and other internet postings including blogs. It applies to the use of social media for both business and personal purposes, during working hours and in your own time to the extent that it may affect the Group. This policy applies regardless of whether social media is accessed using the Group's Information Systems or not.

b. Whilst the Group recognises the benefits which may be gained from appropriate use of social media, it is also important to be aware that it may pose significant risks to the Group. These risks include disclosure of confidential information and intellectual property, damage to the Group's reputation and the risk of legal claims. To minimise these risks, this policy sets out the rules applying to the use of social media.

c. This policy covers all employees and others including consultants, contractors, and casual and agency staff. Breach of this policy may result in disciplinary action including dismissal. Any misuse of social media must be reported to the Group's Information Technology Department. Questions regarding the content or application of this policy may be directed to the Group's Head of Information Technology Department or the Group's Corporate Communications Department or the Group's Talent Success Department.

d. The Group may amend this policy at any time if it considers it appropriate to do so.

5.2 Personal Use of Social Media at Work

a. The Group allows employees to make occasional personal use of social media, so long as it does not involve unprofessional or inappropriate content and does not adversely affect your productivity, or otherwise interfere with your duties to the Group. All use must comply with this policy.

b. The Group may monitor your use of its Information Systems, including use of social media sites, in accordance with the principles set out in this Code of Conduct for Employees.

5.3 Business Use of Social Media

a. If you are required or permitted to use social media sites in the course of performing your duties for or on behalf of the Group, you must ensure that such use has appropriate authorisation and that it complies with the standards set out in this policy.

5.4 Responsible Use of Social Media

a. You must not use social media in a way that might breach any Group policy, any express or implied contractual obligations, legislation, rule or regulatory requirements. Use of social media must comply with:

   i. Harassment Policy (Clause 2);

   ii. Information Technology and Communications Systems Policy (Clause 3); and

   iii. contractual confidentiality requirements.

b. In your use of social media, you must not:

i. make disparaging or defamatory statements about the Group, its employees, clients, customers, or suppliers;

ii. harass, bully or unlawfully discriminate in any way;

iii. use data obtained in the course of your engagement with the Group which in any way breaches the provisions of the Data Protection Policy (Clause 5);

iv. breach copyright belonging to the Group;

v. disclose any intellectual property, confidential or commercially sensitive information relating to the Group or its business; and

vi. make statements which cause, or may cause, harm to the Group's reputation or otherwise be prejudicial to the interests of the Group.

c. You must avoid using social media communications that might be misconstrued in a way that could damage the Group's reputation.

d. You must make it clear in personal postings that you are speaking on your own behalf by writing in the first person and use a personal email address. If you disclose that you are an employee of the Group, you must explicitly state that your views do not represent those of your employer. For example, you could state, "the views in this posting do not represent the views of my employer".

e. Remember that you are personally responsible for what you communicate on social media. Oftentimes, materials published will be widely accessible by the public and will remain accessible for a long time. If you are uncertain or concerned about the appropriateness of any statement or posting, you should discuss it with the Group's Corporate Communications Department before making the post.

f. The contact details of business contacts made during the course of your engagement with Group are regarded as confidential information belonging to the Group. On termination of your engagement, you must provide the Group with a copy of all such information, delete all such details from your personal social networking accounts and destroy any further copies of such information that you may have.

g. Any form of communication found on social media and/or instant messaging shall be considered as a valid form of communication.

6. DATA PROTECTION POLICY

6.1 Introduction

a. The Group believes in the importance of responsible handling of information and the confidentiality of its employees' and other individuals' personal information.

b. The Group holds and processes information about its employees and other individuals for various purposes (e.g., in connection with health and safety, security and monitoring of the Group's premises, and Information Systems).

c. The information and guidelines set out in this policy are important and apply to all employees. You must familiarise yourself with these guidelines and procedures and ensure that you comply with them. Failure to comply with these guidelines and procedures may amount to a disciplinary offence and may constitute Gross Misconduct (see Annex A).

d. We reserve the right to make changes to this policy at any time. Where appropriate, we will notify data subjects of these changes by mail or email.

6.2 Commitment to Data Security

a. All employees share the Group's responsibilities under the data protection legislation to ensure that data from which living individuals can be identified (i.e., personal data), is processed fairly and in accordance with the law, whether this data relates to employees or clients, customers or business contacts. Particular care needs to be taken to ensure the security and integrity of such data, especially sensitive personal data, and employees must ensure that they comply with the Group's latest information technology procedures in that regard.

6.3 Data Protection

a. The Group is committed to complying with the data protection principles and which serve to protect an individual's right to privacy. In summary the Group strives to ensure that personal data is:

   i. processed fairly and lawfully;

   ii. obtained and processed for specified and lawful purposes;

   iii. adequate, relevant and not excessive for those purposes;

iv. accurate and kept up to date;

v. not kept for longer than is necessary;

vi. processed in accordance with an individual's rights under the relevant laws; and

vii. protected by appropriate measures against unauthorised or unlawful processing, accidental loss or destruction.

6.4 Your Personal Data

a. Your personal particulars are solely for administration purposes only and are not used for the basis of hiring.

b. The Group will process personal data about you in accordance with and to the extent permitted by relevant laws. This is for the Group to carry out its legitimate business interests.

c. Your personal data may be kept electronically or in hard copy format. Your personal data may be disclosed or transferred to:

i. other employees of the Group;

ii. other persons as may be reasonably necessary for the purposes of or in connection with your employment; or

iii. as otherwise required or permitted by law.

d. You agree that the Group may, from time to time, post personal data about you on its website for legitimate business purposes. For example, the Group may promote a department's activities on its website and include the name and work contact details of some individuals in that department. You should be aware that this website is, in theory, accessible worldwide.

6.5 Sensitive Personal Data

a. Sensitive personal data is information as to a data subject's racial or ethnic origin, political opinions, religious beliefs or beliefs of a similar nature, physical or mental health condition, sexual life, offences or alleged offences, and information relating to any proceedings for offences committed or allegedly committed by the data subject, including the outcome of those proceedings.

b. You agree that the Group may process sensitive personal data relating to you, in connection with your engagement or the activities of the Group. The Group envisages the need to process sensitive personal data for purposes that include but are not limited to the following:
   i. data relating to the ethnic origin of employees of the Group may be processed for the purposes of equal opportunities monitoring;
   ii. the provision of healthcare, general welfare and monitoring attendance and poor performance; and
   iii. in exceptional circumstances, the Group may need to process information regarding criminal convictions or alleged offences in connection with, for example, any disciplinary proceedings or other legal obligations.

c. You agree that the Group may disclose or transfer these categories of sensitive personal data to other persons outside the Group if it is required or permitted by law to do so.

6.6 Processing

a. Processing, in relation to the Group's use of information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:
   i. organising, adaptation or alteration of the information or data;
   ii. retrieval, consultation or use of the information or data;
   iii. disclosure of the information or data; or
   iv. destruction of the information or data.

6.7 Data Protection Officer

a. The Group's Data Protection Officer is Mr. Brandon Ong. He has overall responsibility for data protection issues. If you have any queries concerning these guidelines and procedures, you may raise them with him. You may contact him using the following email address: dataprotection@charleskeith.com.

6.8 Disclosure of Information

a. The Group relies on the cooperation of its employees in striving to keep personal information confidential. It is important that all employees ensure that:
   i. any personal data which they hold is kept securely; and
   ii. personal data is not disclosed either verbally, in writing, or otherwise, to any unauthorised third party.

b. If you receive telephone enquiries, you must exercise great care before disclosing any personal information (e.g., the address or telephone numbers of employees). You should:
   i. check the caller's identity, to make sure that information is only given to a person who is entitled to it;
   ii. ask the caller to put their request in writing, if you are not sure about the caller's identity and where their identity cannot be checked; and
   iii. ask your immediate supervisor for assistance in difficult situations, as no one should be bullied or otherwise be subjected to under undue influence to disclosing personal information.

c. Personal data must be kept securely and examples of how this may be done include:
   i. keeping the data locked in a filing cabinet, drawer or room; and
   ii. if the data is computerised, ensuring that the data is password protected or kept only on disk which is itself kept securely.

d. Unauthorised disclosure of personal information may result in very serious consequences. It is a disciplinary offence and may constitute Gross Misconduct (see Annex A), leading to summary dismissal. Obtaining or disclosing personal data of another individual or employee without the Group's prior written consent may attract personal criminal liability as a result of a breach of data protection legislations.

6.9 Keeping Information up to date

a. You must ensure that any personal data which you provide to the Group is accurate and up to date. Any change of address or other personal details must be notified to the Group's Talent Success Department.

b. The onus is on all employees to maintain and update any changes to their personal particulars in the Group's Workday system. The Group's Talent Success Department will process any changes to employees' personal particulars once they are updated in the Group's Workday system.

6.10 Manual and Computer Systems

a. You must only process personal data in accordance with the Group's prior written instructions. No one in the Group may, without the prior written authorisation of the Data Protection Officer:
   i. develop a new computer system for processing personal data;
   ii. use an existing computer system to process personal data for a new purpose;
   iii. create a new manual filing system containing personal data; or
   iv. use an existing manual filing system containing personal data for a new purpose.

6.11 Right to Access Personal Data

a. All employees (and any other individuals) have a right under the relevant laws to access personal data relating to themselves which is held by the Group, in both electronic format and manual records, that form part of a "relevant filing system" (which broadly means they are held in a structured way).
b. If you wish to see personal data relating to you, you may submit such request in writing to the Data Protection Officer.
c. The Company will, as far as possible, respond to any such request for access to personal data within 40 calendar days (including public holidays and weekends) of the request.
d. If you find any inaccuracies in the data disclosed, you must immediately inform the Data Protection Officer who will arrange for the necessary amendments to be made.
e. If you receive any written request from an individual for their personal data, you must immediately pass the request to the Data Protection Officer.

7. PUBLIC INTEREST DISCLOSURE (WHISTLEBLOWING) POLICY

7.1 Introduction

a. The Group always conducts its business with the highest standards of integrity and honesty. It expects you to maintain the same standards in everything you do. You are therefore encouraged to report any wrongdoing by the Group or its employees that falls short of these principles.

b. The Group will protect employees who report wrongdoing within the workplace. The Group recognises that you may not always feel comfortable about discussing your concerns internally, especially if you believe that the Group itself is responsible for the wrongdoing. The aims of this policy are:

   i. to ensure that as far as possible you feel able to inform your immediate supervisor about any wrongdoing at work which you believe has occurred or is likely to occur;

   ii. to give guidance on what to do if you have concerns about any wrongdoing; and

   iii. to reassure employees that they can raise any matter that concerns them with the Group in the knowledge that it will be taken seriously, treated as confidential and that no action will be taken against them.

c. This policy applies to all employees and workers engaged with the Group (including managers, directors, agency workers, and contractors).

d. The Group may reinforce this policy at any time if it considers it appropriate to do so.

7.2 When should you use this Policy?

a. You may use the procedure set out below if you have any concerns about wrongdoing at work, including:

   i. criminal offences;

   ii. failure to comply with legal obligations;

   iii. miscarriage of justice;

   iv. health and safety danger;

   v. environmental risk; or

   vi. concealment of any of the above.

b. You do not need to be able to prove the truth of the information you provide under this policy, but you must reasonably believe its disclosure is in the public interest and tends to show some malpractice as outlined above.

c. Complaints relating to your personal circumstances (such as how you have been treated at work) should not generally be made under this policy and should be raised under the appropriate Group policies.

7.3 Whistleblowing Procedure

a. In many cases you may be able to discuss any concerns about any wrongdoing with your immediate supervisor in the first instance. However, where the matter is more serious or you prefer not to raise it with them for any reason, you may contact the Director/Regional Head of the relevant entity or the Group's Talent Success Department at whistleblowing@charleskeith.com.

b. If the matter requires further investigation, such investigation will be carried out and you will be informed of the outcome of the investigations and what, if any, action has been taken.

c. If you remain unhappy about the speed or conduct of the investigation or the way in which the matter has been resolved, you may refer the matter to any member of the Management Committee. When they have investigated your complaint, they will inform you of the outcome of the investigation and what, if any, action has been taken.

d. The Group will not be able to inform you of any matters which would infringe the duties of confidentiality it owes to others.

7.4 Confidentiality

a. The Group encourages you to raise your concerns openly under this policy. However, if you want to raise your concerns confidentially, every effort would be made to maintain confidentiality as far as possible.

b. The Group does not encourage disclosures to be made anonymously. Proper investigation may be more difficult or impossible if the Group cannot obtain further information from you. It is also more difficult to establish whether any allegations made are credible. If you are concerned about possible reprisals, you may contact the Director/Regional Head of your respective entity or the Group's Talent Success Department and appropriate measures will be taken to preserve confidentiality.

7.5 Protection from Detriment

a. The Group undertakes that no employee who makes a *bona fide* report under this procedure will be subjected to any detriment as a result.

b. If you believe you are being subjected to a detriment by any person within the Group as a result of your decision to use the procedure, you must inform the Director/Regional Head of your respective entity or the Group's Talent Success Department immediately and appropriate action will be taken to protect you from any reprisals.

c. To ensure the protection of all our employees, those who make an allegation which they do not reasonably believe to be true or in the public interest, will be liable to disciplinary action in accordance with this policy.

7.6 Proper Reporting

a. The Group is keen to hear any concerns that employees may have about wrongdoing at work and encourages them to use the procedures described above wherever possible.

b. The Group recognises that there may be matters that cannot be dealt with internally and external authorities may need to be involved. Where this is necessary, the Group reserves the right to make such referrals without your consent.

c. Questions regarding this policy, and/or any claims may be directed to the Group's Talent Success Department or the Group's Legal and Compliance Department.

8. ANTI-CORRUPTION POLICY

8.1 Introduction

a. The Group is committed to conducting all its business in an honest and ethical manner. It adopts a zero-tolerance approach to bribery and corruption, and is committed to acting professionally, fairly, and with integrity in all business dealings and relationships wherever it operates.

b. This policy outlines the responsibilities of the Group and those who work for it in relation to the prevention of bribery and corruption. It aims to give guidance and information on recognising and addressing relevant issues.

c. This policy applies to all employees working at all levels and grades, including senior managers, officers, directors, employees (whether permanent, fixed-term or temporary), consultants, contractors, trainees, seconded staff, homeworkers, workers (including casual workers) and agency staff, volunteers, interns, agents, sponsors, or any other person associated with the Group, or its subsidiaries or their employees, wherever located.

d. The Group's contract templates shall include the necessary terms and conditions to ensure the compliance with Group's anti-corruption policy.

e. Individuals may face imprisonment if they are found guilty of offences under the relevant laws. In addition, the Group could be liable to financial penalties, be excluded from tendering for public contracts, and would suffer serious damage to its reputation, if corruption or bribery were to take place. The Group therefore takes its legal obligations in this regard very seriously.

f. All individuals play a key role in ensuring the compliance of this policy. You are expected to familiarise yourself with this policy and act in accordance with it at all times. Any employee who breaches this policy will face disciplinary action, which could result in dismissal for Gross Misconduct (see Annex A). For other individuals and organisations, the Group may terminate any contractual relationship in response to any breach, or suspected breach, of this policy.

g. The Group may reinforce this policy at any time if it considers it appropriate to do so.

8.2 Unlawful Conduct

a. Under the relevant laws, it is a criminal offence to:

   i. bribe another person;

ii. accept a bribe;

iii. bribe a foreign public official; or

iv. fail to prevent bribery within a commercial organisation.

b. A bribe is an inducement or reward offered, promised or provided in order to gain any commercial, contractual, regulatory or personal advantage through the improper performance of a business or employment-related function or activity. Performance is improper if it is not in good faith, is not impartial, or if it is in breach of an expectation of trust.

c. An offence arises under the respective countries' laws regardless of whether the unlawful act of bribery is committed in the home country or elsewhere.

8.3 Gifts and Hospitality

a. This policy does not prohibit normal and appropriate hospitality (given and received) to or from third parties. Genuine hospitality and promotional activity which aims to improve the image of the Group, improve presentation of products or services, or establish good relations is not prohibited by the relevant laws unless there is an intention to induce improper performance of an activity or function. You must immediately declare all gifts received from a third party to the Group's Administration Department. Records of all gifts declared will be kept for auditing purposes.

b. Formal pre-approval must be obtained from Executive Director and above prior to gifting or entertaining public officials.

8.4 Donations

a. The Group only makes charitable donations that are legal and ethical under local laws and practices. No donation must be offered or made without the prior written approval of the Group's Legal and Compliance Department (legal@charleskeith.com) or the Group's Talent Success Department.

8.5 Prohibited Conduct

a. You must not, through any means or conduct:

i. give, promise to give, or offer, a payment, inducement, gift or hospitality with any expectation or hope that it may or may not result in a business advantage arising from the improper performance of a relevant function or business activity;

ii. accept payment from a third party that you know or have reason to suspect is offered with the expectation that it will result in a business advantage in consequence of the improper performance of a relevant function or business activity;

iii. accept a gift or hospitality from a third party if you know or have reason to suspect that it is offered or provided with an expectation that it could or will result in a business advantage in consequence of improper performance of a relevant function or business activity by the Group;

iv. give, promise to give, or offer, a payment, inducement, gift or hospitality to a government official, agent or representative to "facilitate" or expedite a routine procedure;

v. threaten or retaliate against another worker who has refused to commit a bribery offence or who has raised concerns under this policy; or

vi. engage in any other activity that might lead to a breach of this policy or the spirit of this policy.

8.6 Third Parties

a. The Group may be liable for third parties who commit any act of bribery or corruption. The definition of a third party is broad. It covers individuals and organisations who perform services for the Group and may include agents, distributors, consultations and others acting on the Group's behalf.

b. For this reason, third parties who act on the Group's behalf must be provided with a copy of this policy and will be expected to operate in accordance with it at all times.

c. If you are instructing third party representatives to act on behalf of the Group, you must bear in mind that they can potentially expose the Group to significant risks. You are responsible for ensuring that the necessary precautions are taken to minimise such risks. You may discuss appropriate steps with the Group's Legal and Compliance Department.

8.7 Facilitation Payments and Bribes

a. The Group does not make, and will not accept, facilitation payments or bribes of any kind. Facilitation payments are typically small, unofficial payments made to secure or expedite a routine government action by a government official. Bribes are typically payments made in return for a business favour or advantage.

b. This is governed by the respective home jurisdictions' laws, where it is illegal to make or receive facilitation payments or bribes.

c. If you are asked to make a payment, you must consider what the payment is for and whether the amount requested is proportionate to the goods or services provided. You must ask for a receipt which details the reason for the payment. If you have suspicions, concerns or queries regarding a payment, you must raise these with the Group's Legal and Compliance Department.

d. You must avoid any activity that might lead to, or suggest, that a facilitation payment or bribe will be made or accepted by the Group.

8.8 Your Responsibilities

a. All those working for, or under the control of the Group are responsible for the prevention, detection and reporting of bribery and other forms of corruption. You are required to avoid any activity that might lead to, or suggest, a breach of this policy.

b. You must notify the Group's Legal and Compliance Department as soon as possible if you know or have reason to suspect that a breach of this policy has occurred, or may occur in the future. For example, if a client or potential client offers you something to gain a business advantage, or indicates to you that a gift or payment is required to secure their business.

8.9 Record-Keeping

a. The Group maintains accurate books, records and financial reporting. These records will be transparent and will accurately reflect each underlying transaction.

b. You must immediately declare and keep a written record of all hospitality or gifts accepted or offered. All expense claims relating to hospitality, gifts or expenses incurred to third parties must be submitted in accordance with the Group's expenses policy and specifically record the reason for the expenditure.

c. All accounts, invoices, memoranda and other documents and records relating to dealings with third parties, such as clients, suppliers and business contacts, must be prepared and maintained with strict accuracy and completeness. No accounts must be kept off-book to facilitate or conceal improper payments.

8.10 Reporting Concerns

a. You must raise concerns about any issue or suspicion relating to this policy as soon as possible. If you are unsure whether a particular act constitutes bribery or corruption, or if you have any other queries, these must be raised with the Group's Legal and Compliance Department. You must follow the procedure contained in the Whistleblowing Policy (Clause 6).

b. If you are offered a bribe by a third party, are asked to make one, have reason to suspect that this may happen in the future, or have reason to believe that you are a victim of another form of unlawful activity, you must report it to the Group's Legal and Compliance Department immediately.

c. Employees who refuse to accept or offer a bribe, or those who raise concerns or report another's wrongdoing, are sometimes worried about possible repercussions. The Group wishes to encourage openness and will support anyone who raises genuine concerns in good faith under this policy, even if they turn out to be mistaken.

d. You will not suffer any detriment if you refuse to take part in bribery or corruption, or if you report such conduct in good faith. If you believe that you have suffered any such treatment, you may inform the Group's Legal and Compliance Department immediately.

8.11 Training and Communication

a. The Group will ensure that employees receive appropriate training in relation to this policy. The level and frequency of training may vary depending on the nature of the position held. The Group will ensure that its zero-tolerance approach to bribery and corruption is communicated to all suppliers, contractors and business partners at the outset of any business relationship and as appropriate thereafter.

8.12 Enforcement and Responsibility

a. The Management Committee has overall responsibility for ensuring that this policy complies with the Group's legal and ethical obligations, and that all those under the Group's control comply with it.

b. The Group's Legal and Compliance Department has primary, day-to-day responsibility for implementing this policy, and for monitoring its use and effectiveness and dealing with any queries on its interpretation.

c. Management at all levels are responsible for ensuring that those reporting to them are made aware of and understand this policy and are given adequate and regular training. The management has specific responsibilities to adhere to appropriate standards in the way they conduct themselves and to lead by example.

8.13 Monitoring and Review

a. The Group's Legal and Compliance Department will monitor the effectiveness and review the implementation of this policy regularly, considering its suitability, adequacy and effectiveness. Any improvements identified will be made as soon as possible. Internal control systems and procedures will be subject to regular audits to provide assurance that they are effective in countering bribery and corruption.

b. You are encouraged to comment on this policy and suggest ways in which it might be improved. Comments, suggestions and queries may be addressed to the Group's Legal and Compliance Department.

8.14 Key Risk Areas

a. The Group has identified the particular risks set out below. The following is an illustrative list of issues, and is not intended to be exhaustive, which may give rise to concern. If you encounter these or other relevant concerns, you must report them promptly to the Group's Legal and Compliance Department:

   i. you become aware that a third party engages in, or has been accused of engaging in, improper business practices;

ii. you learn that a third party has a reputation for paying bribes, or requiring that bribes are paid to them, or has a reputation for having a "special relationship" with foreign government officials;

iii. a third party insists on receiving a commission or fee payment before committing to sign up to a contract, or carrying out a government function or process;

iv. a third party requests payment in cash and/or refuses to sign a formal commission or fee agreement, or to provide an invoice or receipt for a payment made;

v. a third party requests that payment is made to a country or geographic location different from where the third party resides or conducts business;

vi. a third party requests an unexpected additional fee or commission to "facilitate" a service;

vii. a third party demands excessive entertainment or gifts before commencing or continuing contractual negotiations or provision of services;

viii. a third party requests that a payment is made to "overlook" potential legal violations;

ix. a third party requests that you provide employment or some other advantage to a friend or relative;

x. you receive an invoice from a third-party that appears to be non-standard or customised;

xi. a third party insists on the use of side letters or refuses to put terms agreed in writing;

xii. the Group is invoiced for a commission or fee payment that appears large given the service stated to have been provided;

xiii. a third party requests or requires the use of an agent, intermediary, consultant, distributor or supplier that is not typically used by or known to the Group; or

xiv. you are offered an unusually generous gift or offered lavish hospitality by a third party.

9. HEALTH AND SAFETY POLICY

9.1. Introduction

a. This policy applies to all employees, agency and casual workers.

b. This policy is intended as a statement of current Group policy and its commitment to provide and maintain safe and healthy working conditions, equipment and systems of work for all employees, and to provide such information, training and supervision as needed for this

purpose. The Group is committed to giving equal priority to health, safety and welfare of its employees as to all other aspects of the Group's business. The Group recognises its responsibility for the health and safety of non-employees who may be affected by its activities.

c. The policy will be kept up to date, particularly as the business changes in nature and size. To ensure this, the policy and the way in which it has been implemented will be reviewed every year. The Group will ensure that all revisions are brought to the notice of all employees.

9.2. The Group's Commitment to Health and Safety

a. By law, it is the joint responsibility of the directors and employees to maintain high standards of health and safety. These mutual objectives can only be achieved with the active cooperation and participation of all concerned.

b. The directors will, as far as is reasonably practicable:

i. provide and maintain healthy and safe working conditions in accordance with the relevant statutory requirements;

ii. provide all necessary information, instruction, training and supervision for all employees, including additional safety training where appropriate;

iii. provide and maintain all necessary safety devices and protective equipment and supervise their use;

iv. set an example in good health and safety behaviour;

v. conduct the Group's business undertakings in such a way as to ensure that persons not in the Group's employment, who may be affected thereby, are not exposed to health and safety risks;

vi. maintain a constant and ongoing interest in all aspects of health and safety, in particular by:

- conducting regular health and safety inspections;
- stimulating joint consideration of health and safety matters;
- introducing and monitoring health and safety procedures; and
- appointing a Safety Advisor, who reports to the Group's Building Maintenance Department.

9.3. Responsibility of Employees and other Workers

a. The Group expects and requires that all employees:

i. work safely and consider the safety of others at all times;

ii. report all related incidents, whether injury is caused or not;

iii. report all unhealthy or unsafe working conditions or situations;

iv. cooperate with management when investigating incidents or situations;

v. adhere to the Group's health and safety rules and regulations;

vi. comply with the statutory health and safety requirements;

vii. cooperate with management on safety training programmes; and

viii. observe the Group's no-smoking policy in all areas of the business.

b. It is the responsibility of all employees to:

i. comply with the Group's health and safety policy;

ii. take all reasonable care for their own safety, and the health and safety of others who may be affected by their acts at work;

iii. cooperate insofar as is necessary to ensure that any legal duty or requirement imposed on the Group or any person by or under any of the relevant statutory provisions shall be complied with;

iv. be prepared to undergo any health and safety training deemed necessary by management;

v. report any defective equipment to their immediate supervisor;

vi. maintain a high standard of cleanliness at the workplace and throughout their use of toilets and other amenities;

vii. report to their immediate supervisor, all accidents and dangerous occurrences whether injuries have been sustained or not;

viii. alert their immediate supervisor if they experience any symptoms (whether relating to their physical or mental health) which could be caused by their working environment or conditions;

ix. report for treatment any injury they suffer, however small, and ensure that their immediate supervisor is informed of such injury; and

x. in the event that any employee is in doubt with regards to health and safety matters, they should consult their immediate supervisor immediately.

9.4. Reporting the Incident

a. Employees involved directly or as a witness must report the incident to their immediate supervisor immediately.

b. Complete an incident report form within 24 hours. The form should include:

i. date, time and location of the incident;

ii. names of individuals involved;

iii. description of the incident and potential causes; and

iv. any immediate actions taken.

c. All incidents will be logged and tracked by the Group's Talent Success Department.

d. The supervisor will conduct an initial investigation to identify immediate causes and take corrective actions.

e. The Group's Talent Success Department will review the incident report and may conduct a more detailed investigation.

f. The investigation should include:

i. interviews with involved parties and witnesses;

ii. review of workplace conditions and equipment; and

iii. analysis of any patterns or recurring issues.

g. The log of incidents with root cause and corrective actions documents shall be reported to the Management Committee.

9.5. Organisation

a. Prime responsibility for health and safety lies with the Management Committee. The Management Committee has delegated the management of health and safety matters to the Group's Building Maintenance Department, the Group's Talent Success Department, or the landlord, where this responsibility falls onto that of our landlord.

ANNEX A

Group Code of Conduct for Employees

Gross Misconduct: The following are examples of gross misconduct under this Code of Conduct for Employees, which if violated, the employee may be subject to disciplinary actions that may lead to dismissal:

a. Theft of any kind
b. Frequent lateness and/or leaving work early without approval
c. Absence without a valid reason
d. Inciting conflict with another employee repeatedly
e. Fighting, violent behaviour and causing disturbance at workplace
f. Integrity issues, insulting another, slander and/or affecting the unity of employees
g. Malingering
h. Bringing or consuming of unauthorised goods, including but not limited to, narcotics, chemicals, vapes or drugs
i. Wilful damage of the Group's property
j. Being intoxicated while on duty
k. Harassment of any kind
l. Acts of racism
m. Insubordination
n. Falsely providing personal information to the Group
o. Altering or falsifying Group documents with the use of Group stamps or monies
p. Negligence leading to the direct economic loss to the Group
q. Trading with unauthorised sellers
r. To obtain gratification as an inducement to or reward for an act related to suppliers or contractors
s. Using business transactions for personal gain
t. Acts which may cause disrepute to the Group
u. Being found guilty of other serious disciplinary offences
v. Any conduct that infringes any applicable laws of respective countries and jurisdictions