Associate Consultants Policies and Procedure Pack

V1.1 February 2021

Introduction

This pack contains CSR Management Groups policies and procedures which are applicable to Associate Consultants.

Please read this document carefully. By signing the Associate Consultant Agreement for the Provision of Contracted Services you agree to comply with all of the requirements of this document while conducting work for CSR Management Group.

This document has been approved and authorised by:

Name: Ian Dodd

Position: Managing Director

Date: 11/02/2021

Due for Review by: 11/02/2021

Signature: 

Bonus and Finder's Fee Policy

V1.0 November 2020

We believe in rewarding cooperation and have developed the following policy to reward our Contractors for their hard work:

Bonuses

We will pay a discretionary bonus for the following activities:

a) Contribution to a successful bid, whether the Contractor is selected to work on the project or not.
b) Performance of the Contractor based on successful completion of assigned project work on time, on budget and of high quality.

Bonuses will be paid either at the end of a project or at CSR Management Group's financial year end. All bonuses are subject to the financial performance of the project and the company.

Finder's Fees

A finder's fee of 1% of contract value will be paid to any Contractor who refers CSR Management Group to any project which it was not yet aware of and subsequently wins, whether or not the Contractor supports the bid and/or works on the project.

Anti-bribery and corruption policy and procedure

V1.0 November 2020

1. Zero-tolerance to bribery

It is the policy of CSR Management Group Limited and its associates, including joint venture companies (the Group or CSR Management Group) to conduct its business with honesty and integrity. CSR Management Group has a zero-tolerance approach to bribery and corruption in all its business dealings and relationships. CSR Management Group expects the same from its employees and in its relationships with all those with whom it does business.

2. What does the policy apply to?

The Anti-Bribery and Corruption Policy and Procedure (the Policy and Procedure) applies to CSR Management Group, its directors, officers, employees and temporary and contract workers.

CSR Management Group will endeavour to ensure that people and businesses who perform services for us, for example, agents, representatives, contractors, consultants and advisers, when acting on our behalf and when conducting business in partnership with us comply with the principles of this Policy and Procedure.

This Policy and Procedure applies irrespective of the country in which business is being conducted and sets minimum Group standards. Where there are differences between the local law and the Policy and Procedure, you must apply either the Policy and Procedure or the local law, whichever sets the highest standard of behaviour.

3. Why does the Policy and Procedure matter to you?

Most countries have laws that prohibit bribery and corruption and a number of countries have implemented laws that make bribery even outside its borders a criminal offence.

This Policy and Procedure is designed to help you understand your obligations and comply with the law. If you fail to follow the Policy and Procedure you put yourself, your colleagues and CSR Management Group at risk of committing a criminal offence.

You are personally responsible for:

- ethical and professional conduct and for compliance with the Policy and Procedure;
- obtaining advice and guidance where necessary; and
- reporting all suspicions of criminal activity, breaches of this Policy and Procedure, and/or any ethical or professional misconduct, whether committed personally or by others.

Anyone who is found to be engaging in bribery or corruption, or otherwise breaching this Policy and Procedure, will be subject to disciplinary action.

The Policy and Procedure contains general advice on good ethical and business practice, supported by detailed sections dealing with identified areas of high-risk business activity.

4. What is bribery and corruption?

Acts of bribery or corruption are designed to influence another in the performance of their duties and to act in a way contrary to how their employer, their organisation or the public would expect them to act.

Criminal offences can be committed by offering, promising, giving, requesting, agreeing to accept or receiving a bribe.

Bribes usually take the form of improper payments or personal "commissions". They can, however, take on many different shapes and forms, such as gifts, hospitality, entertainment, loans, holidays, favours, the provision of services, reimbursement of travel and other expenses, secret rebates, charitable or political donations, job offers, scholarships, and unfair advantages for family or friends in respect of training or employment opportunities (secondments, work experience, trainee positions, internships or permanent positions).

Most countries in the world have made it an offence to bribe their own public officials[1]; many have also made it an offence to bribe a foreign public official. For example, in the UK a bribery offence is committed by offering or giving anything of value to a non-UK public official with the intention of influencing that individual to obtain or retain a business advantage.

5. No bribes or facilitation payments

5.1 Principle

Those employed or engaged by CSR Management Group must never solicit, accept, agree to receive, promise, offer or give a bribe which includes facilitation payments, kickbacks and other improper payments or benefit for any reason or in any form.

[1] A “public official” for this purpose is an officer or employee of a government (e.g. civil servants in national and local government); employee of public bodies such as the police and local regulators; employees of the judiciary; employees of the armed forces; an officer or employee of a “public international organisation” or any person acting in an official capacity for or on behalf of such public international organisation (e.g. the United Nations, the World Bank, the European Commission, etc.); an employee of a company or other business entity in which a governmental body has an ownership interest and/or over which such governmental body may, directly or indirectly, exercise a dominant influence (e.g. state owned); a political party or a member of a political party or a candidate for political office; and any person known or suspected to be a close family member or associate of any of the above, or companies who are controlled by close family members or associates of any of the above.

5.2 Rules

Do	Don't
• Ensure you understand your obligations under the Policy and Procedure and operate at all times ethically and within the law. If uncertain, seek advice (see "What to do if you have a query or concern"). • Remain alert to the risks of bribery and corruption. • Use caution and obtain required approvals when offering, giving or receiving gifts or entertainment (see "Prohibited and Permitted Gifts and hospitality"). • Seek further guidance immediately if you are being asked to do something which makes you uncomfortable, or which you suspect may be illegal (see "What to do if you have a query or concern"). • Consider the legal, professional, or ethical codes which apply to the parties you are dealing with. • Report any concerns you have about improper conduct or corruption activity immediately (see "What to do if you have a query or concern").	• Solicit, accept, agree to receive, promise, offer or give bribes or kickbacks, or make facilitation payments. This applies to dealings with private businesses and persons, dealings with foreign or domestic government officials or employees, and to international and domestic business. • Use agents or other third parties to solicit, accept, agree to receive, promise, offer or give bribes or kickbacks, or make facilitation payments indirectly on behalf of CSR Management Group. • Use other forms of giving or receiving as a substitute for a "bribe", for example, political or charitable donations, gifts or hospitality. • Be persuaded by others to do something which you suspect might be illegal. • Ever attempt to induce anyone else to do something illegal, even if "everyone else is doing it". • Make any charitable donation on behalf of CSR Management Group without the written consent (including by email) of the relevant CSR Management Group Executive Team member. Consent will only be given where the donation is not dependent on, nor made in order to win a business deal or gain any other commercial advantage. • Make any political donations on behalf of CSR Management Group. • Use or allow to be used any CSR Management Group assets or resources for political purposes. • Attempt to circumvent our financial control systems, make 'off the book payments' or secret payments • Ignore or fail to report any concerns you have about improper conduct or corruption activity or otherwise "look the other way".

5.3 Guidance

Some of the common indicators of corruption are as follows:

- Abnormal cash payments.
- Payments being made to an individual who works for a client. This would include both payments made directly to the individual or to a company associated with the individual.
- Payments being made through third party countries which are unconnected to the goods or services being provided.
- Private meetings with public contractors or companies when tendering for contracts.
- Lavish gifts being given or received.
- An unexplained insistence by clients for work to be completed by a particular technician or laboratory.
- Bypassing normal tendering or other contract procedures.

No distinction is made between bribes and so-called "facilitation" payments, which are also prohibited. A facilitation payment includes a small payment to a public official, which is not officially required, to enable or speed up a process which it is the official's job to arrange (e.g. a work permit). We also seek to ensure that third parties do not make facilitation payments on our behalf (see "Use of third parties").

A bribe includes "kickbacks" which are also prohibited. A kickback is a form of bribery in which a percentage of the revenues from a contract or other financial award is illicitly returned to the person awarding that contract or benefit.

Bribes may take the form of charitable contributions or educational sponsorships. When assessing whether to consent to any charitable or educational donations which are proposed to be made on behalf of CSR Management Group, the relevant Executive Team member must provide written approval and will require that:

- donations must be given to a charitable organisation and not to an individual, or to an educational establishment on behalf of a particular student and not directly to the student concerned;
- charitable contributions are only permitted to charities that are registered under the local country's laws;
- a risk-based approach must be adopted and where necessary background checks and due diligence are undertaken on the charity itself and on its managers and representatives; and
- the recipient of the money and the purpose for which it is to be applied must be known.

Bribes can be concealed in the form of political donations. There have been cases where overseas foreign officials have tried to use such contributions as a bargaining tool.

6. Do not falsify test results or certificates

6.1 Principle

CSR Management Group and those employed or engaged by it must never falsify test results or certificates. The integrity of CSR Management Group, and those employed or engaged by it in producing test results and certificates, is of the upmost importance. Any actions to falsify such results or certificates may do irreparable harm to CSR Management Group's reputation and are strictly forbidden.

6.2 Rules

Do	Don't
• Conduct all tests and issue test and other certificates in accordance with industry standards, accreditation body regulations and legitimate client requirements. • Keep appropriate records of test results. • Report test results accurately. • Review or amend test results for genuine technical reasons and never as a result of commercial pressure or as a result of a bribe (see "No Bribes or facilitation payments"). • Report any concerns you have about improper test results or certificates immediately (see "What to do if you have a query or concern").	• Solicit, accept or agree to receive bribes or kickbacks in return for test results or certificates (see "No Bribes or facilitation payments"). • Falsify or improperly amend test results or certificates. • Ignore or fail to report any concerns you have about improper test results or certificates or otherwise "look the other way".

7. Comply with the highest ethical standards when engaging with governments

7.1 Principle

Whenever CSR Management Group conducts business or otherwise engages with national or local governments, government agencies, public bodies, public international agencies, state owned companies, and employees and officials of such bodies and organisations, our employees and anyone engaged by or on behalf of CSR Management Group must apply the highest ethical standards.

CSR Management Group requires full compliance with all applicable laws and regulations; this includes certain special requirements associated with government transactions.

7.2 Rules

Do	Don't
• Ensure you understand and abide by applicable laws and regulations relating to work with governments, particularly special requirements associated with government contracts and transactions. • Ensure that any third party engaged on behalf of CSR Management Group understands the CSR Management Group policy on working with government officials and agrees to comply with it. • Be truthful and accurate when dealing with government officials and agencies and cooperate courteously with officials conducting government or regulatory enquiries or investigations. • Seek advice if you are unsure about what to do when working with government officials (see "What to do if you have a query or concern"). • If asked to assist with a government or regulatory agency enquiry or investigation you must always seek advice before responding (see "What to do if you have a query or concern".) • Report any concerns you have about improper conduct or corruption activity immediately (see "What to do if you have a query or concern").	• Do not make illicit or secret payments or transfers of any value to government officials. • Deviate from contractual requirements without written approval from both sides. • Use agents or other third parties to do anything indirectly on behalf of CSR Management Group which you would not be permitted to do yourself, this includes making any payments or transfers of items of value through intermediaries, or to a third party, while knowing or suspecting that all or a portion of the payment will go directly or indirectly to a government official. • Attempt to induce a local or government official to do something illegal or attempt to or exert improper influence on government officials. • Ignore or fail to report any concerns you have about improper conduct or corruption activity or otherwise "look the other way". • Mislead any government or regulatory official. • Attempt to obstruct in any manner an authorised government official in the proper conduct of their duties or attempt to hinder another person from providing accurate information.

8. Prohibited and permitted gifts and hospitality

8.1 Principle

CSR Management Group's employees and anyone engaged by or on behalf of CSR Management Group must never accept, offer or give gifts or hospitality to influence the business decision-making process or cause others to perceive an influence. The use of gifts and hospitality in this manner constitutes an improper payment for the purposes of CSR Management Group's policy on bribes and facilitation payments.

CSR Management Group has a clear position which forbids the solicitation of gifts and hospitality and ensures that the circumstances in which modest gifts and hospitality are offered, given or accepted are restricted to those which are appropriate and compliant with applicable laws and regulations.

When deciding whether to offer, give, or receive gifts and hospitality consider the underlying purpose. If the purpose is to induce or persuade the recipient to act improperly you should not proceed. If you feel you will be improperly influenced by a gift or hospitality offered to you, do not accept it.

8.2 Rules

Do	Don't
• Before offering or accepting any gifts or hospitality, you must obtain approval from your General Manager or relevant functional manager for any gift or hospitality. • Any gift or hospitality worth GBP £200 (or the equivalent amount in local currency) or above per recipient must be also approved in writing (including email) by the relevant CSR Management Group Executive Team member. • Make gifts or offer hospitality only in compliance with this policy and applicable laws and regulations. • Be aware of the potential conflicts of interest if you accept gifts or hospitality. • Make the criteria for inviting guests to hospitality events clear and internally transparent. Consider extending the invitation to the most senior people in the target organisation and respect their decision to send whoever they want. • Seek advice if you are unsure about the giving or receiving of gifts or hospitality (see "What to do if you have a query or concern"). • Report any concerns you have about improper conduct or corruption activity immediately (see "What to do if you have a query or concern").	• Give, offer, accept or request the following: ○ Gifts or hospitality which you know or suspect to be illegal. ○ Cash or cash equivalents. ○ Personal services, provided personally, rather than in a business context, unless such services are pursuant to a proper arm's length business transaction. ○ Loans from or to persons that CSR Management Group does business with. ○ Travel and/or accommodation costs for family members unless approved by the relevant CSR Management Group Executive Team member. ○ Events or meals where the business partner is not present. ○ Gifts or hospitality during periods when important decisions regarding the award or retention of business or a business advantage are being made with the business partner or when test results or certificates are being provided. ○ Be embarrassed to politely decline any offer by referring to this policy. This will be understood by the business counterparty who in most cases will be subject to similar rules. ○ Gifts or entertainment you would feel uncomfortable explaining to your work colleagues, your family or the media. • Do not solicit gifts or hospitality.

8.3 Guidance

- The occasional acceptance or offer of modest gifts and hospitality may be a legitimate contribution to good business relationships. Permitted gifts and hospitality generally include:
    - Corporate gifts of low value generally bearing our logo (diaries, umbrellas, calendars etc.).
    - Gifts of low value (not including cash) given during the festive seasons of the year.
    - Working breakfasts, lunches or evening meals, provided they are on a modest scale and on an occasional basis.
    - Occasional invitations to corporate hospitality events or industry conferences, seminars or trade shows, and modest hospitality incidental to such events.
- There may be times when refusing to accept gifts or hospitality from a business partner or declining to provide them would be considered discourteous. Nevertheless, compliance with 8.2 overrides any such other considerations.
- Sometimes your General Manager or relevant functional manager may decide that it is appropriate for a gift to be accepted on behalf of CSR Management Group or your team, rather than being retained by you personally.
- You need to exercise caution when providing gifts or hospitality to business partners or prospective business partners or their representatives, particularly where these individuals have discretion over the allocation of work.
- Gifts or hospitality provided to a partner, spouse or relative of a business should generally not be provided,
- You need to exercise extra caution when providing gifts or hospitality to government officials (including employees or representatives), particularly where these individuals have discretion over the allocation of work.
- CSR Management Group employees and representatives should consider the following questions before accepting or offering a gift or hospitality:
    - Could my acceptance or offer lead to an obligation or imply an obligation?
    - Is this gift, hospitality or entertainment event a "sweetener" connected to the award or retention of business or other business advantage?
    - Is this gift, hospitality or entertainment event a "reward" for the award or retention of business or other business advantage or the provision of test results or certificates?
    - Does this gift or hospitality seem excessive in value?
    - Am I in danger of breaching any applicable laws or regulations?
    - Are there any potential adverse reputational implications in the type of gift or entertainment being accepted or given? Would my colleagues be unhappy to see CSR Management Group reported in the press in connection with this gift or hospitality event?

If the answer to any of these questions is "yes", the gift or hospitality should not be offered or accepted. If you are not clear how to answer these questions you should seek advice (see "What to do if you have a query or concern").

9. Use of third parties

9.1 Principle

CSR Management Group expects third parties to act in accordance with the Policy and Procedure when acting on behalf of or otherwise representing CSR Management Group. Third parties presenting an increased risk of bribery and corruption should be subject to due diligence.

CSR Management Group has a clear position which forbids the use of third parties to undertake activity prohibited under the Policy and Procedure.

9.2 Rules

Do	Don't
• Follow the due diligence process (see below for details). • Engage third parties in good faith, with awareness of the associated risks and in CSR Management Group's best interests. • Adopt a risk based approach when engaging a third party to act on behalf of or represent CSR Management Group or a client. • Exercise caution when dealing with third parties such as agents, consultants and other intermediaries, especially when they are helping to market or promote CSR Management Group's business, or engaging with governments or government officials. • Manage the activities of third party relationships to ensure compliance with the Policy and Procedure and other applicable legal and regulatory obligations by those that act on behalf of or represent CSR Management Group. • Report any concerns you have about improper conduct or corruption activity immediately (see "What to do if you have a query or concern").	• Use agents or other third parties to do anything indirectly on behalf of CSR Management Group which you would not be permitted to do yourself. • Allow third parties to represent CSR Management Group or our clients in high risk situations (e.g. in dealings with government officials) without proper supervision. • Make payments through or to a third party (or any other intermediary) if you know or have reason to suspect that all or part of the payment will be used for a purpose which breaches the Policy and Procedure. • Ignore or fail to report any concerns you have about improper conduct or corruption activity or otherwise "look the other way".

9.3 Guidance

- All third parties which act on behalf of or represent CSR Management Group must act in accordance with the Policy and Procedure when they do business with us and if they do business with a third party on our behalf.

- A risk-based approach must be adopted when engaging third parties to act on behalf of or represent CSR Management Group, with a view to assessing the corruption risk before engaging with them.
- The following documents must have been read, understood and acknowledged by signing an Associate Consultant Agreement for the Provision of Contracted Services:
    - Ethics and Code of Conduct Agreement; and
    - Agreement for the Provision of Contracted Services OR a Pre-Qualification Questionnaire

  prior to engaging with:
    - Third parties which provide a sales type function for CSR Management Group or which help us to secure new business;
    - Third parties which are described as an "agent" or "intermediary";
    - Third parties which are paid on the basis of a commission or success fee;
    - Third parties which interact with government officials on our behalf, for example visa and customs agents;
    - Third parties assessed by the person considering the third party's appointment to present an increased bribery risk. Relevant factors for determining an increased bribery risk include:
        - requests by a public official or business decision maker for us to use the services of a specific third party;
        - any indication that the third party may have a conflict of interest;
        - where it is proposed that the third party is paid in a country that is different to where the services are to be performed; or
        - high remuneration tied to the outcome of a transaction.
- Due diligence should either be carried out in advance of each significant new contract or transaction involving the third party or, where due diligence has been conducted in the previous 24 months, the previously completed Ethics & Compliance Questionnaire should be checked and may be relied on so long as there is no reason to consider the risk profile to have changed. A Third-Party Authorisation Form must be completed prior to any significant new contract or transaction with the third party.
- Copies of the Ethics and Code of Conduct Agreement, Agreement for the Provision of Contracted Services and Pre-Qualification Questionnaires are retained by Ian Dodd, Managing Director.
- The following principles must be applied when engaging a third party on behalf of CSR Management Group or on behalf of a client:
    - payments must be reasonable and reflect rationally the value of the services to be provided by the third-party;
    - the third party should have a proven track record in the business discipline and geographical location concerned;
    - you should exercise particular caution if a third party is referred by government officials or is known to have political affiliations;
    - the services to be rendered by the third party must be legitimate;
    - any personal interest which you have in any agreement or transaction must be disclosed; and
    - payments should not be made offshore unless there are genuine and legitimate business reasons for doing so.

10. What to do if you have a query or concern

If you have a query regarding how the Policy and Procedure applies to you, then you should contact your General Manager or relevant functional manager for guidance.

If you believe that the Policy and Procedure has been or is being breached, you have an obligation to report your concerns to someone who can deal with the situation. You must not ignore your concerns. In the first instance you should raise any concern with your General Manager or relevant functional manager. Your manager will make an initial assessment of any potential breaches, and/or any ethical or professional misconduct. Where it appears that a breach may have occurred, your manager will report the matter to the relevant CSR Management Group Executive Team member.

If you feel that your General Manager or relevant functional manager has not addressed your concern, or you prefer not to raise it with them for any reason, you should report the matter to Ian Dodd, Managing Director responsible for Anti-bribery and Corruption. Alternatively, you may wish to discuss the matter with Protect, the Whistleblowing Charity. This is a UK managed and staffed service, where colleagues can seek advice on concerns before they are reported to CSR Management Group for appropriate action.

11. Changes to this policy

This Policy will be reviewed every two years and, where appropriate, to reflect any changes to legislation or in our methods or practices.

Ethics & Code of Conduct Agreement

V1.0 November 2020

The overall aim of CSR, Sustainability and ESG approaches is to give confidence to all stakeholders that an organisation understands their sustainability impacts and is acting to minimise those or have a positive impact. This extends to our people and those whom complete work on our behalf. It is therefore imperative that CSR Management Group maintain the highest degree of public confidence and trust that is established by professional, competent and ethical conduct on all our projects.

This agreement includes a commitment to the principles for inspiring confidence in the our consulting services:

- Confidentiality;
- Impartiality;
- Openness;
- Responsiveness to complaints;
- Anti-bribery and corruption.

CSR Management Group insists on honesty, integrity and fairness in all aspects of its business and expects the highest standards of professionalism and ethical conduct to be maintained in all its activities. All CSR Management Group employees, sub-contractors, subsidiaries, associated companies and authorised representatives have a commitment to ensure that they uphold the principles for inspiring confidence to all stakeholders in the delivery of consultancy services.

General

When working for or on behalf of CSR Management Group I confirm that I will:

- act with fairness, honesty and integrity at all times and comply with the CSR Management Group Anti-Bribery and Corruption Policy and Procedure;
- act within the applicable laws and legislation;
- undertake activities in accordance with CSR Management Group procedures and guidelines and to comply with applicable accreditation requirements;
- work safely, upholding the CSR Management Group health & safety policies and practices;
- communicate clearly, effectively and openly;
- be accountable for my actions;
- treat colleagues, clients and other stakeholders with an appropriate level of respect and consideration;
- respect matters of faith, conscience and diversity in their widest sense;
- avoid behaviour that could be regarded as harassment, bullying, exploitation or intimidation;
- safeguard the reputation and assets of the company;

- co-operate fully with any investigation in the event of any alleged breach of this code of conduct.

Confidentiality

When working for or on behalf of CSR Management Group I confirm that:

- I will maintain the confidentiality of all information obtained or created during the provision of services;
- I shall not disclose any information about a particular certified client or individual to a third party without written approval from CSR Management Group;
- If I intend to place any client information in the public domain I will obtain written approval from CSR Management Group;
- If required by law or authorised by contractual arrangements (i.e. Accreditation body) to release confidential information I shall obtain written approval from CSR Management Group before release of such information;
- I will maintain equipment and facilities that ensure the secure handling of confidential information

Impartiality

Being impartial and being perceived to be impartial is critical for CSR Management Group to deliver services that provide confidence. All CSR Management Group employees, sub-contractors, subsidiaries, associated companies and authorised representatives shall not allow commercial, financial or other pressures to compromise impartiality.

When working for or on behalf of CSR Management Group I confirm that:

- I will avoid situations where a threat to impartiality or objectivity arises, or where potential conflict of interest could exist, or be seen to exist;
- I will declare any conflicts of interest where I have been employed, provided consultancy for or connected with a client in any way. All declarations will be made regardless of the time period.
- I will not be involved in with a client, including consulting, audit, report review, complaints, disputes or appeals and certification decision making for a minimum period of 1 year after any connection with a client through CSR Management Group.
- I will declare in writing immediately to CSR Management Group any situation known to me that presents me or CSR Management Group with a conflict of interest. Examples of such situations include but are not limited to:
    - Self-interest threats: threats that arise from a person or body acting in their own interest to
    - benefit themselves;
    - Self-review threats: threats that arise from a person or body reviewing the work done by
    - themselves. An individual/organisation auditing the system(s)/product(s) of a client to whom the
    - individual/organisation has provided consultancy would be a self-review threat;

- Subjectivity threats: Threats that arise when personal bias overrules objective evidence;
- Familiarity threats: threats that arise from a person or body being too familiar with or trusting of another person e.g. An auditor or staff member developing a relationship with an applicant /certified organisation that affects the ability to reach an objective judgement;
- Intimidation threats: threats that prevent person(s) from acting objectively due to fear of a person/organisation/interested party;
- Financial threats: threats that arise from sources of revenue.

Openness

Where required by CSR Management Group you must disclose information requested to ensure the openness and transparency required for maintaining the integrity and credibility of our services.

Responsiveness to complaints and stakeholder concerns

Parties expect to have complaints/stakeholder concerns investigated and if these are found to be valid, should have confidence that the complaints/stakeholder concerns will be appropriately addressed and that a reasonable effort will be made to resolve the complaints/stakeholder concern. Effective responsiveness to complaints/stakeholder concerns is an important means of protection for CSR Management Group, its clients and other stakeholder to address errors, omissions or unreasonable behaviour.

When working for or on behalf of CSR Management Group I confirm that I will be open to investigation of complaints/stakeholder concerns. If these are found to be valid, I will allow such complaints to be appropriately addressed and will assist in the resolution as required.

Anti-Bribery and Corruption

CSR Management Group does not engage in bribery or corruption in any form and has a zero tolerance approach to breaches of this policy, whether it involves private individuals or public officials. The Anti-Bribery and Corruption Policy and procedure applies in all jurisdictions where we do business - irrespective of any applicable local or international legal or regulatory obligations. Notwithstanding this, CSR Management Group is committed to comply with all anti-bribery and corruption legislation and regulation applicable to its businesses and people.

In line with the requirements of the Anti-Bribery and Corruption Policy, when working for or on behalf of CSR Management Group I confirm that I must never solicit, accept, agree to receive, promise, offer or give a bribe, facilitation payment, kickback or other improper payment.

If you require clarification on any aspect of this agreement you should seek the advice of Ian Dodd, Managing Director.

Complaints Procedure

V1.0 November 2020

CSR Management Group takes complaints very seriously. This procedure applies to all aspects of our business including, but not limited to, Chain of Custody and Payments:

We shall ensure that complaints received regarding our conformity to policies, procedures, certifications, commitments and contracts are adequately considered, including the following:

a) acknowledge receipt of the complaint to the complainant within two (2) weeks of receiving the complaint;
b) investigate the complaint and specify our proposed actions in response to the complaint within three (3) months. If more time is needed to complete the investigation, the complainant and any relevant stakeholders, including certification bodies, shall be notified;
c) take appropriate actions with respect to complaints and any deficiencies found in processes that affect conformity to requirements;
d) notify the complainant and other stakeholders, such as certification bodies, when the complaint is considered to be successfully addressed and closed.

All complaints shall be addressed to Ian Dodd, Managing Director, and submitted by email to info@csrmanagement.org.

Staff Privacy Policy

V1.1 November 2020

What is the purpose of this document?

You have legal rights about the way your personal data is handled by us, CSR Management Group Limited. We are committed to protecting the privacy and security of your personal information.

This privacy notice describes how we collect and use personal information about you during and after your working relationship with us. It applies to all 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.

During your employment or engagement by us, we collect, store and process personal data about you. To comply with the law and to maintain confidence in our business, we acknowledge the importance of correct and lawful treatment of this data.

It is important that you read this notice, along with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you. This gives you information about how and why we are using such information. All people working in or with our business are obliged to comply with this policy when processing personal data.

Our Role

We are a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. Data protection legislation requires to give you the information contained in this privacy notice.

Data protection principles

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

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

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 "special categories" of more sensitive personal data that require a higher level of protection.

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

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- Date of birth.
- Gender.
- Marital status and dependants.
- Next of kin and emergency contact information.
- National Insurance number.
- Bank account details, payroll records and tax status information.
- Salary, annual leave, pension and benefits information.
- Start date.
- Location of employment or workplace.
- Copy of driving licence.
- 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).
- Employment records (including job titles, work history, working hours, training records and professional memberships).
- Compensation history.
- Performance information.
- Disciplinary and grievance information.
- Photographs.

We may also collect, store and use the following "special categories" of more sensitive personal information:

- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions.
- Trade union membership.
- Information about your health, including any medical conditions, health and sickness records.
- Genetic information and biometric data.
- Information about criminal convictions and offences.

How is your personal information collected?

Usually 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.

We will collect additional personal information during work-related activities throughout the period of you working for us.

How we will use information about you

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

- Where we need to perform the contract that applies to our working relationship.
- Where we need to comply with a legal obligation.
- Where it is necessary for our legitimate interests (or those of 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:
- Where we need to protect your interests (or someone else's interests).
- Where it is needed in the public interest or for official purposes.

Situations in which we will use your personal information

We need all the categories of information in the list above (see *The kind of information we hold about you*) 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 for our legitimate interests or those of third parties, provided that your interests and fundamental rights do not override those interests. The situations in which we will process your personal information are listed below:

- Making a decision about your recruitment or appointment.
- Determining the terms on which you work for us.
- Checking you are legally entitled to work in the UK.
- Paying you and, if you are an employee or we are under a legal obligation, deducting tax and National Insurance contributions.
- Providing the following benefits to you: Bonus
- Administering the contract that applies to our working relationship with you.
- Business management and planning, including accounting and auditing.
- Conducting performance reviews, managing performance and determining performance requirements.
- Making decisions about salary reviews and compensation.
- Assessing qualifications for a particular job or task, including decisions about promotions.

- Gathering evidence for possible grievance or disciplinary hearings.
- Making decisions about your continued employment or engagement.
- Making arrangements for the termination of our working relationship.
- Education, training and development requirements.
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.
- Ascertaining your fitness to work.
- Managing sickness absence.
- Complying with health and safety obligations.
- To prevent fraud.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- To conduct data analytics studies to review and better understand employee retention and attrition rates.
- Equal opportunities monitoring.

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

If you fail to provide personal information

If you do not provide certain information when we ask for it, we may not be able to perform the contract that applies to our working relationship with you (such as paying you or providing a benefit), or we may not be able to comply with our legal obligations (such as to ensure the health and safety of our workers).

Change of purpose

We will only use your personal information for the purposes that we have collected it for, unless we need to use it for another reason and that reason is reasonable and 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 that allows us to do so.

We may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or allowed by law.

How we use particularly sensitive personal information

"Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the situations below:

- In limited circumstances, with your clear written consent.
- Where we need to carry out our legal obligations and in line with our data protection

policy or other policy that applies to such information.

- Where it is needed in the public interest, such as for equal opportunities monitoring and in line with our data protection policy or other policy that applies to such information.
- Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.

Very occasionally, 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.

Our obligations as an employer

We will use your particularly sensitive personal information in the following:

- We will use information relating to leaves of absence, which may include sickness absence or family-related leave and related pay, to comply with employment and other laws.
- 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.
- We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

Do we need your consent?

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 give you full details of the information that we would like and the reason we need it, so that you can consider carefully 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.

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 or other policy that applies to such information.

Very occasionally, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary 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.

We do not envisage that we will hold information about criminal convictions.

Automated decision-making

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We can use automated decision-making in the following circumstances:

- Where we have notified you of the decision and given you 21 days to request a reconsideration.
- Where it is necessary to perform the contract with you and appropriate measures are in place to safeguard your rights.
- In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

If we make an automated decision based on any particularly sensitive personal information, we must have either your explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights.

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

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.

Data sharing

We may have to share your data with third parties, including third-party service providers and other entities in the group.

We require third parties to respect the security of your data and to treat it in accordance with the law.

We may transfer your personal information outside the EU.

If we do, you can expect a similar degree of protection in respect of your personal information.

Why might we share your personal information with third parties?

We may 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.

Which third-party service providers process your personal information?

"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
- Accounting
- Cloud Services
- Web Hosting Services

How secure is your information with third-party service providers and other entities?

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.

What about other third parties?

We may share your personal information with other third parties, for example in the context of the possible sale or restructuring of the business. We may also need to share your personal information with a regulator or to otherwise comply with the law.

Transferring information outside the EU

We may transfer the personal information we collect about you to countries outside the EU to perform our contract with you.

To ensure that your personal information does receive an adequate level of protection we have put in place the following appropriate measures to ensure that your personal information is treated by those third parties in a way that is consistent with and which respects the EU and UK laws on data protection: Approved Suppliers Procedure, for

example, includes a check on GDPR policy for services outside the EU. If you require further information about this or these protective measures, it is available upon request.

Data security

We have put in place measures to protect the security of your information. Details of these measures are available upon request.

Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

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. Details of these measures will be provided upon request.

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

How long will you use my information for?

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. Details of retention periods for different aspects of your personal information are available in our Data Retention Policy which is available upon request.

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.

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 our Data Retention Policy or applicable laws and regulations.

Rights of access, correction, erasure, and restriction

Your duty to inform us of changes

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 relation to personal information

Under certain circumstances, by law you have the right to:

- 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.
- 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.
- Request that your personal information is erased. This allows 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 stop processing personal information where we are relying on a legitimate interest and there is something about your situation that makes you want to object to processing on this ground.
- 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.
- Request the transfer of your personal information to another party.

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 our head office in writing.

No access fee usually required

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.

What we may need from you

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.

Right to withdraw consent

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 our head office. 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.

Data Protection Officer

We are not required to appoint a Data Protection Officer to oversee compliance with this privacy policy. If you have any questions about this privacy policy or how we handle your personal information, please contact the Managing Director. 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.

Changes to this policy

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.

If you have any questions about this privacy notice, please contact ian@csrmanagement.org.

Internet and Email Acceptable Use Policy

V1.1 November 2020

Use of the internet and email by employees, workers and contractors (herein referred to as employees) of CSR Management Group is permitted and encouraged where such use supports the goals and objectives of the business.

However, CSR Management Group has a policy for the use of the internet and email whereby employees must ensure that they:

- comply with current legislation
- use the internet and email in an acceptable way
- do not create unnecessary business risk to the company by their misuse of the internet and email

Unacceptable behaviour

In particular the following is deemed unacceptable internet use or behaviour by employees:

- visiting internet sites that contain obscene, hateful, pornographic or otherwise illegal material
- using the computer to perpetrate any form of fraud, or software, film or music piracy
- using the internet to send offensive or harassing material to other users
- downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence
- hacking into unauthorised areas
- publishing defamatory and/or knowingly false material about CSR Management Group, your colleagues and/or our customers on social networking sites, ‘blogs’ (online journals), ‘wikis’ and any online publishing format
- revealing confidential information about CSR Management Group in a personal online posting, upload or transmission - including financial information and information relating to our customers, business plans, policies, staff and/or internal discussions
- undertaking deliberate activities that waste staff effort or networked resources
- introducing any form of malicious software into the corporate network

The following behaviour by an employee is considered unacceptable email use:

- use of company communications systems to set up personal businesses or send chain letters
- forwarding of company confidential messages to external locations
- distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal

- distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered as harassment
- accessing copyrighted information in a way that violates the copyright
- breaking into the company's or another organisation's system or unauthorised use of a password/mailbox
- broadcasting unsolicited personal views on social, political, religious or other non-business-related matters
- transmitting unsolicited commercial or advertising material
- undertaking deliberate activities that waste staff effort or networked resources
- introducing any form of computer virus or malware into the corporate network

Company-owned information held on third-party websites

If you produce, collect and/or process business-related information in the course of your work, the information remains the property of CSR Management Group This includes such information stored on third-party websites such as webmail service providers and social networking sites, such as Facebook, Twitter and LinkedIn.

Monitoring

CSR Management Group accepts that the use of the internet and email is a valuable business tool. However, misuse of these facilities can have a negative impact upon employee productivity and the reputation of the business.

In addition, all of the company's internet and email resources are provided for business purposes. Therefore, the company maintains the right to monitor the volume of internet and network traffic, together with the internet sites visited. The specific content of any transactions will not be monitored unless there is a suspicion of improper use. The company also maintains the right to examine any systems and inspect any data recorded in those systems.

In order to ensure compliance with this policy, the company also reserves the right to use monitoring software in order to check upon the use and content of emails. Such monitoring is for legitimate purposes only and will be undertaken in accordance with a procedure agreed with employees.

Sanctions

Where it is believed that an employee has failed to comply with this policy, they will face the company's disciplinary procedure. If the employee is found to have breached the policy, they will face a disciplinary penalty ranging from a verbal warning to dismissal. The actual penalty applied will depend on factors such as the seriousness of the breach and the employee's disciplinary record.

Changes to this policy

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.

If you have any questions about this privacy notice, please contact ian@csrmanagement.org.

Data Protection Policy

V1.1 November 2020

Data Protection Officer

CSR Management Group are not required to have a Data Protection Officer. Our Managing Director named above assumes all associated responsibilities.

Commencement of this policy

This Policy shall be deemed effective as of 13/11/2020 however it will not have effect retrospectively and will apply only to matters occurring after this date.

Our specific data protection measures

In relation to our use of personal data CSR Management Group take the following measures:

- Encryption: CSR Management Group encrypt the following data in transit or at rest:
    - Employee Computers
    - Back up Hard Drive
    - Website Hosting Service
    - Mobile Phone
    - Cloud Services
    - Website traffic
- Erasure, destruction and or deletion: Digital deletion or physical shredding.
- Transmission of hard copies: Signed for service with tracking
- Storage of emails and email content: Cloud services, webhosting services, company computers and backup hard drive.
- Access of third parties: Approved Suppliers List and Data Access Procedure
- Storage of hardcopies: Unless legally required to retain hard copies of documents, all are digitised and hardcopies destroyed as above. Hardcopies that have to be stored are locked in a locker onsite.
- Storage of electronic copies: Electronic copies of personal data are stored and encrypted as above.
- Sharing: Approved Suppliers List and Data Access Procedure
- Sub-processing: Approved Suppliers List and Data Access Procedure
- Viewing on systems: Data Access Procedure
- Viewing on devices: Data Access Procedure
- Passwords: All employees use a password manager approved by the company

Our use of personal data and our purpose

CSR Management Group may collect, hold and/or process the following personal data:

- Name: To enable us to refer to you by name when contacting you.
- Job Role: To ensure CSR Management Group only contact you with information CSR Management Group think is relevant to your job role.

- Employer: So CSR Management Group know who you work for and can make sure CSR Management Group only contact organisations CSR Management Group believe will benefit from our services.
- Email Address: This is our primary form of direct communication for our mailing list, first point of contact following a referral and communication of proposals and general business information once a contract has been signed.
- Phone Number: CSR Management Group may follow up with prospective clients once an initial email contact has been made, during the proposal development or following a proposal submission. Calls may also be used during contract delivery.

Section A: Overview

1. **The reason for this policy**

1.1 You have legal rights with regard to the way your personal data is handled.

1.2 In the course of our business activities CSR Management Group collect, store and process personal data about our customers, suppliers and other third parties and therefore, in order to comply with the law and to maintain confidence in our business, CSR Management Group acknowledge the importance of correct and lawful treatment of this data.

1.3 All people working in or with our business are obliged to comply with this policy when processing personal data.

2. **Introduction**

2.1 This policy and any other documents referred to in it sets out the basis on which CSR Management Group will process any personal data CSR Management Group collect from data subjects, for example, customers and business contacts, or that is provided to us by data subjects or other sources.

2.2 In this policy when CSR Management Group say “you’ or “your” CSR Management Group are generally referring to the data subjects unless the context requires otherwise.

2.3 It also sets out our obligations in relation to data protection under the General Data Protection Regulation 2016 (“the **GDPR Rules**”).

2.4 This policy sets out rules on data protection and the legal conditions that must be satisfied when CSR Management Group obtain, handle, process, transfer and store personal data.

2.5 CSR Management Group agree to ensure that all of our directors, employees, consultants and agents comply with this policy.

2.6 CSR Management Group aim to ensure the correct, lawful, and fair handling of your personal data and to respect your legal rights.

3. **The meaning of key Data Protection terms**

3.1 **data** is information which is stored electronically, on a computer, or in certain paper-based filing systems.

3.2 **data subjects** for the purpose of this policy include all living individuals about whom CSR Management Group hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

3.3 **personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

3.4 **data controllers** are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Act. CSR Management Group are the data controller of all personal data used in our business for our own commercial purposes.

3.5 **processing** is any activity that involves use of personal data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

4. Summary of the Data Protection Principles

This Policy aims to ensure compliance with the GDPR Rules. The GDPR Rules sets out the following principles with which any party handling personal data must comply. All personal data must be:

a) **Processed fairly and lawfully** – it must be processed fairly and lawfully and it must be processed - in relation to you as the data subject - in a transparent manner

b) **Processed for limited purposes and in an appropriate way -** the purposes for which it is collected must be explicit, specified and legitimate

c) **Adequate, relevant and not excessive for the purpose**

d) **Accurate** – as well as being accurate it must be kept up to date with inaccurate data deleted

e) **Not kept longer than necessary for the purpose**

f) **Processed in line with data subject's rights**

g) **Security** – there must appropriate technical or organisational measures to ensure appropriate security

In addition, personal data must not be transferred outside the European Economic Area (the "**EEA**") **without adequate protection.**

Section B: Data Protection Principles

5. **Notifying Data Subjects**

5.1 As part of complying with the principles in para 4 above, if you provide us with personal data CSR Management Group will always try to tell you:

5.1.1 the purpose or purposes for which CSR Management Group intend to process that personal data

5.1.2 the types of third parties, if any, with which CSR Management Group will share or to which CSR Management Group will disclose that personal data

5.1.3 how you can limit our use and disclosure of their personal data

5.1.4 if CSR Management Group receive personal data from other sources.

6. **Lawful, Fair, and Transparent Data Processing**

The GDPR Rules are not intended to prevent the processing of personal data but to ensure that it is done fairly and without adversely affecting your rights. The processing of personal data is lawful if one (or more) of the following applies:

a) **(consent)** the data subject has consented for a specific purpose;

b) **(contract**) if the data subject requests the processing with a view to entering into a contract or the processing is necessary for the performance of a contract

c) **(legal obligation)** if the processing is necessary for the compliance with a legal obligation to which the data controller is subject

d) **(protection)** processing is necessary to protect your vital interests or those of another natural person

e) **(public interest)** it is in the public interest for a task to be carried out which requires such processing, or the task is to be carried out as a result of the exercise of any official authority held by the data controller;

f) **(legitimate interests)** for the legitimate interest of the data controller or the party to whom the personal data is disclosed.

7. **Processed for limited purposes and in an appropriate way**

7.1 In the course of our business, CSR Management Group may collect and process the personal data set out above. This may include personal data CSR Management Group receive directly from you (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data CSR Management Group receive from other sources (including, for example, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

7.2 CSR Management Group will only process personal data for the specific purposes set out above or for any other purposes specifically permitted by the GDPR Rules. CSR Management Group will notify those purposes to you when CSR Management Group first collect the personal data or as soon as possible thereafter.

8. **Adequate, Relevant and not excessive for the purpose**

CSR Management Group will only collect and process personal data for the specific purpose(s) set out above.

9. **Accuracy of Data and Keeping Data Up To Date**

CSR Management Group will keep your personal data accurate and up-to-date. CSR Management Group will check its accuracy regularly. When CSR Management Group find inaccurate or out-of-date data CSR Management Group will take reasonable steps to amend or erase that data.

10. **Timely Processing**

CSR Management Group will only keep your personal data for a period of time which CSR Management Group judge is relevant and necessary taking into account the purpose(s) of collecting the personal data which are specified above.

11. **Processing that is secure**

In addition to the measures above:

11.1 CSR Management Group will make sure that the personal data CSR Management Group collect is securely kept and CSR Management Group stop unauthorised processing and prevent its loss, destruction or damage

11.2 CSR Management Group will ensure that only people who are authorised to use personal data can access it and that CSR Management Group have entry controls to our premises and systems, lockable desks and cupboards for confidential personal data and destruction of hard copy documents and digital storage devices

11.3 all authorised persons must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

Section C: Data Subject Rights

12. You, as a data subject, have the right to information about:

    a) who CSR Management Group are

    b) the purpose(s) of collecting your personal data and the legal basis for collecting it and what our legitimate interest is for processing your personal data

    c) the categories of personal data collected and where is to be transferred, especially if outside the EEA

    d) the length of time CSR Management Group hold personal data (or, where there is no predetermined period, details of how that length of time will be determined)

    e) your rights as a data subject including your right to withdraw your consent to processing, the right to complain to the Information Commissioner and also things such as details of any legal requirement for processing personal data that may exist and any automated decision-making that CSR Management Group carry out.

    CSR Management Group will try to provide this information when CSR Management Group collect the personal data or, if CSR Management Group collect the personal data from another party, when CSR Management Group communicate with you after the personal data is received.

13. **Data Subject Access**

    13.1 You may request access to any data held about you by us (a subject access request ("**SAR**")

    13.2 CSR Management Group reserve the right to charge reasonable fees for onerous or repetitive requests.

    13.3 Data subjects must make a formal request for information CSR Management Group hold about them. This must be made in writing.

    13.4 When receiving telephone enquiries, CSR Management Group will only disclose personal data CSR Management Group hold on our systems if the following conditions are met:

    a) CSR Management Group will check the caller's identity to make sure that information is only given to a person who is entitled to it.

    b) CSR Management Group will suggest that the caller put their request in writing if CSR Management Group are not sure about the caller's identity and where their identity cannot be checked.

14. **Accuracy of personal data: right to rectification**

    14.1 CSR Management Group will do our best to ensure that all personal data held about you is accurate and complete. CSR Management Group ask that you notify us of any changes to information held about you.

    14.2 You have the right to request that any incomplete or inaccurate information held about you is rectified and to lodge a complaint with us and the Information Commissioner's Office.

14.3 CSR Management Group will respond to requests to rectify within one month.

15. **Right to be forgotten**

You have the right to request the deletion or removal of personal data however requests for erasure can be rejected in certain circumstances.

16. **Right to restriction of Processing**

You can block the processing of your personal data. This means CSR Management Group may be able to store it, but cannot process it further without consent. Restricting data is required where the accuracy of data is challenged - but only until the accuracy has been verified.

17. **Right to data portability**

17.1 If you have provided personal data to us you have the right to transfer it from us to someone else.

17.2 If you request it, CSR Management Group may be required to transmit the data directly to another organisation if feasible. CSR Management Group must respond without undue delay and within one month, or two months if the request is complex.

18. **The right to object**

You have a right to object to the processing of your data. CSR Management Group must stop processing unless CSR Management Group can demonstrate a legal ground for the processing.

19. **Automated decision-making**

19.1 You have the right not to be subject to a decision based on automated processing and it produces a legal effect or other significant effect on you.

19.2 You can request human intervention where personal data is processed using automated decision-making and can ask for an explanation of the decision to use automated decision-making.

20. **Profiling**

If CSR Management Group use your personal data for profiling purposes:

a) CSR Management Group will give you information fully explaining the profiling which will be carried out including its importance and the likely results of that profiling;

b) CSR Management Group will make sure that appropriate mathematical or statistical procedures will be used;

c) CSR Management Group will implement technical and organisational measures which are required to minimise the risk of mistakes and to enable such mistakes to be easily corrected; and

d) CSR Management Group will make sure that all personal data processed by us for profiling purposes will be kept secure so as to avoid discriminatory effects resulting from such profiling.

Section D: Our Other Obligations

21. **How CSR Management Group deal with personal data internally**

21.1 CSR Management Group will:

a) train our employees in relation to our responsibilities under the GDPR Rules

b) ensure that only appropriately trained, supervised and authorised personal have access to personal data held by us; and

c) regularly evaluate and review our collection and processing of personal data and the performance of employees and third parties working on our behalf to ensure that it is in accordance with the GDPR Rules.

21.2 CSR Management Group will keep internal records of personal data that CSR Management Group collect and process including, in relation to that personal data, details of the categories, any transfers, our security measures, our purpose of collection and the duration of retention of that personal data. CSR Management Group will also retain details of all third parties that either collect your personal data for us or that CSR Management Group use to process your personal data.

21.3 CSR Management Group will carry out privacy impact assessments as required by law.

22. **Transferring personal data to a country outside the EEA**

CSR Management Group may transfer personal data to countries outside of the EEA however CSR Management Group will ensure that the transfer is:

a) to a place that the EU has judged to provide adequate levels of protection for personal data

b) to a place that provides adequate safeguards under either an agreement with a public body, rules that bind companies or standard data protection clauses adopted by the EU or some other form of approved code of conduct approved by a supervisory authority or certification or other contractual clauses or regulatory provisions

c) necessary for the performance of a contract between you and us or with a view to creating that contract

d) made with your consent

e) necessary for important public interest reasons, legal claims, to protect your vital interests

23. **Notification of personal data security breach**

23.1 If a personal data security breach occurs, CSR Management Group will manage and respond to it effectively in accordance with GDPR and it must be reported immediately to our Managing Director.

23.2 CSR Management Group will notify the Information Commissioners Office (**ICO**) and any data subject of personal data security breaches to the extent CSR Management Group are required to do so by GDPR.

23.3 If disclosure is not required by GDPR, CSR Management Group will nevertheless investigate closely all the circumstances surrounding the breach

and examine the seriousness of the breach and the benefits that might be obtained by disclosure (such as limiting risks of fraud) and CSR Management Group will give careful consideration to any decision to notify the ICO or you, especially if your rights and freedoms as data subjects are affected.

Data Retention Policy

V1.1 November 2020

Introduction

This data retention policy sets out the obligations of CSR Management Group Limited ("us/we/our") and the basis upon which CSR Management Group shall retain, review and destroy data held by us, or within our custody or control.

This policy applies to our entire organisation including our officers, employees, agents and sub-contractors and sets out what the retention periods are and when any such data may be deleted.

CSR Management Group are registered under the Information Commissioner's Office under registration number:

ZA783815

Objectives

It is necessary to retain and process certain information to enable our business to operate. CSR Management Group may store data in the following places:

- our own servers;
- any third-party servers;
- potential email accounts;
- desktops;
- employee-owned devices (BYOD);
- potential backup storage; and/or
- our paper files.

This policy applies equally to paper, electronic media and any other method used to store personal data. The period of retention only commences when the record is closed.

CSR Management Group are bound by various obligations under the law in relation to this and therefore, to comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully in respect of their personal data under the General Data Protection Regulation ("the Regulation").

The Regulation defines "personal data" as any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to

the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

This Policy sets out the procedures that are to be followed when dealing with personal data and how CSR Management Group aim to comply with the Regulation in so far as it is possible. In summary, the Regulation states that all personal data shall be:

a) processed lawfully, fairly, and in a transparent manner in relation to the data subject;

b) collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of the data subject;

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The Fourth and Fifth Data Protection Principles require that any data should not be kept longer than necessary for the purpose for which it is processed and when it is no longer required, it shall be deleted and that the data should be adequate, relevant and limited for the purpose in which it is processed.

With this in mind, this policy should be read in conjunction with our other policies which are relevant such as our data protection policy and IT security policy.

Security and Storage

All data and records are stored securely to avoid misuse or loss. CSR Management Group will process all personal data CSR Management Group hold in accordance with our IT Security Policy.

CSR Management Group will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal

data will only be transferred to a data processor if there is agreement by them to comply with those procedures and policies, or if there are adequate measures in place.

Examples of our storage facilities are as follows:

- Cloud Storage Services Provided by Microsoft and Google
- Employee and contractor owned devices
- Company backup hard drive which is not connected to the internet
- Web hosting services
- Email marketing service

CSR Management Group will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

Confidentiality means that only people who are authorised to use the data can access it.

Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.

Availability means that authorised users should be able to access the data if they need it for authorised purposes.

Retention Policy

Data retention is defined as the retention of data for a specific period of time and for back up purposes.

CSR Management Group shall not keep any personal data longer than necessary but acknowledge that this will be dependent on the different types of documents and data that CSR Management Group have responsibility for. As such, our general data retention period shall be for a period of three years, unless otherwise specified in another agreement. Our specific data retention periods are set out below:

All data will be subject to the following processing: Collection, recording, organisation, structuring, storage, retrieval, use, disclosure by transmission, dissemination, erasure and destruction.

All data is processed in order to contact businesses and individuals with information CSR Management Group Ltd believes is relevant or of interest to the recipient.

Data Type Specific information is as follows:

- **Customers**
    - Type of data subject: Individuals and organisations
    - Type of recipient to whom personal data is transferred: Stakeholders with contractual requirements, Web Hosting Service and Cloud Services
    - Retention period: 3 years from last use
- **Business contacts**
    - Type of data subject: Individuals
    - Type of recipient to whom personal data is transferred: Potential clients for proposals and referrals, Web Hosting Service and Cloud Services
    - Retention period: 3 years from last use
- **Employees**
    - Type of data subject: Individuals
    - Type of recipient to whom personal data is transferred: Clients for whom they are working, proposals for potential clients. External organisations for work references, events and awards, Web Hosting Service and Cloud Services
    - Retention period: 3 years from termination
- **Contractors**
    - Type of data subject: Individuals
    - Type of recipient to whom personal data is transferred: Potential clients for proposals and referrals, Web Hosting Service and Cloud Services
    - Retention period: 3 years from last use
- **Potential employees**
    - Type of data subject: Individuals
    - Type of recipient to whom personal data is transferred: Other potential employers, Web Hosting Service and Cloud Services
    - Retention period: 1 year from last use
- **Mailing List Subscribers**
    - Type of data subject: Individuals
    - Type of recipient to whom personal data is transferred: Email marketing service, Web Hosting Service and Cloud Services
    - Retention period: 3 years from last use or unsubscription

All above data will be reviewed at least annually for accuracy and minimisation.

From time to time, it may be necessary to retain or access historic personal data under certain circumstances such as if CSR Management Group have contractually agreed to do so or if CSR Management Group have become involved in unforeseen events like litigation or business disaster recoveries.

Destruction and Disposal

Upon expiry of our retention periods, CSR Management Group shall delete confidential or sensitive records categorised as requiring high protection and very high protection, and CSR Management Group shall either delete or anonymise less important documents.

Our Managing Director is responsible for the continuing process of identifying the records that have met their required retention period and supervising their destruction. The destruction of confidential, financial, and personnel-related records shall be securely destroyed electronically or by shredding if possible. Non-confidential records may be destroyed by recycling.