JANINE GRANT
CONSULTING
RESEARCH. STRATEGY. ADVOCACY. MANAGEMENT

OPERATIONS MANUAL

2021

OPERATIONS MANUAL

Purpose.

This Operations Manual outlines the policies, procedures and processes used by our company in undertaking our work.

Scope.

This Manual applies to all our employees and consultants regardless of employment agreement or rank.

Human Resources.

Personal appearance.

All staff must follow our dress code when attending the office for work, or when representing our company at events.

Employees should be clean and well-groomed. Grooming styles dictated by religion and ethnicity aren't restricted. Clothing choices should project professionalism. Clothes that are too revealing or could be considered culturally inappropriate aren't allowed. Employees must avoid clothes with stamps or logos that are offensive or inappropriate.

Our company's official dress code is "smart casual", though we may change our dress code in special cases. For example, we may require staff to wear semi-formal attire for an event. An employee's position may inform their dress code. For example, if employees frequently meet with clients or prospects, they should conform to a business dress code.

When an employee disregards our dress code, a line manager may ask their staff to return home to change into something more appropriate. Employees may face more severe consequences up to and including termination if: i) Their appearance causes irreparable damage, like loss of a major client; ii) They repeatedly violate our dress code.

Leave and absenteeism.

Leave Types.

Employees are entitled to all leave categories as determined by the legislation of the country they have been engaged in, as well as any additional entitlements that may be stipulated in their employment contract. Leave types may include annual leave, sick leave, compassionate leave, or parental leave. Details are provided in the employment contract.

Consultants contracted by Janine Grant Consulting are not employees of the company and are not entitled to benefits beyond those stipulated in their Memorandum of Understanding.

Hours of Work.

Employees should follow their agreed schedules. We can make exceptions for occasions that prevent employees from following standard working hours (8 hours per day), or days (Monday-Friday, unless working days in the country they work in vary). But, generally, we expect employees to be punctual when coming to and leaving from work.

Harassment.

We are committed to maintaining a workplace that is free of harassment, so our employees can feel safe and happy. We will not tolerate anyone intimidating, humiliating or sabotaging others in our workplace. We also prohibit willful discrimination based on age, sexual orientation, ethnicity, racial, religion or disability.

This workplace harassment policy applies to all employees, contractors, public visitors, customers, and anyone else whom employees come into contact with at work. Harassment includes bullying, intimidation, direct insults, malicious gossip and victimization. We can't create an exhaustive list, but here are some instances that we consider harassment:

a. Sabotaging someone's work on purpose.
b. Engaging in frequent or unwanted advances of any nature.
c. Commenting derogatorily on a person's ethnic heritage or religious beliefs.
d. Starting or spreading rumors about a person's personal life.
e. Ridiculing someone in front of others or singling them out to perform tasks unrelated to their job (e.g. bringing coffee) against their will.

Sexual harassment is illegal in many of the countries in which we work, and we will seriously investigate relevant reports. If an employee is found guilty of sexual harassment, their contract will be terminated.

If you are being harassed, whether by a colleague, customer or vendor, you may choose to talk to any of these people: i) Offenders. If you suspect that an offender doesn't realize they are guilty of harassment, you could talk to them directly in an effort to resolve the issue. This tactic is appropriate for cases of minor harassment (e.g. inappropriate jokes between colleagues), though this approach should be avoided with customers or stakeholders; ii) Your manager; iii) the company's Executive Director. If customers, stakeholders or team members are involved in your claim, you may reach out to your manager. Your manager will assess your situation and may contact HR or the Executive Director to resolve if appropriate.

Punishment for harassment depends on the severity of the offence and may include counseling, reprimands, suspensions or termination.

Performance management.

For employees.

Key Performance Indicators should be set for each employee at the start of each calendar year and reviews should be carried out annually. All discussions should be documented and saved at the time. All performance issues should be raised with the company's Executive Director as soon as possible, so they are aware of any remedial actions in place.

For consultants and other subcontractors.

The performance of consultants and other subcontractors is monitored by the staff member assigned to manage their contract. Communication with consultants and subcontractors should be open and frequent while they are undertaking their work. Staff are required to provide both clear instructions regarding expectations, and reasonable feedback with regard to performance, in order to ensure deliverables are produced to a high standard. All technical deliverables consultants and subcontractors are responsible for producing are peer reviewed by the company's advisory board prior to submission to the client. In a worst-case scenario where a consultant/subcontractor has been given fair warning and been unable to improve their work standards and fulfil their obligations, Consultant and subcontractor contracts allow for termination, should a consultant or subcontractor fail to meet reasonable expectations with regard to their Work Agreement.

Travel.

When travel for an assignment is required, consultants are entitled to reimbursable travel costs, including flights, per diems (rate agreed within individual contracts) and visa costs if necessary. All receipts for flights and boarding passes must be submitted (electronic copy is acceptable) with consultant invoices.

Consultants are responsible for their own travel and health insurance and must ensure they meet the entry requirements, including proof of insurance and up-to-date vaccinations of countries where they are traveling to undertake an assignment for Janine Grant Consulting.

Employees of the company who need to travel for corporate (non-contract-based work) reasons are entitled to reimbursement for flights, hotels, visa costs, and a standard per diem rate of USD 60/day.

Communications.

Internal communications.

Communication is central to performance of our work, whether in person, verbally or via email. When it comes to internal communications, the following two principles should be applied:

- **Transparency**: Always strive for open communication in all directions (i.e. from leaders to employees, from employees to leaders, and between employees).
- **Inclusivity**: All employees should be informed, engaged, and heard, regardless of their work environment, language preferences, or other needs.

All staff are responsible for taking an active role in promoting effective and efficient internal communications, and managers are responsible for ensuring that messages are communicated to their teams in a timely manner. They are also responsible for communicating employees' feedback to relevant leaders. Employees are responsible for exercising good judgment regarding the tone and content of email communications.

Blogging and social media.

We respect the right of employees and consultants to represent themselves and share their opinions and thoughts on social media networks. Key dos and don'ts of social media usage are outlined below, as a way to protect our company brand:

- Respect other people's privacy. Always ask permission before posting photos of other people or sharing any other information.
- Be careful about security. Don't disclose travel information or business and meeting locations. Don't put photos of locations that you are working at. This may involve disabling geolocation tags.
- Don't disparage other companies, competitors and services.
- If posting to websites or other public forums about the work you are undertaking for our company, the posting must contain a disclaimer stating that the opinions expressed are strictly your own and not necessarily those of our company.

The security of our company and clients is essential. Some useful instructions for ensuring the security of your social media accounts are as follows:

- Remember that everyone can see your messages, updates and dialogue, even if you are writing for private purposes only, and this information will be available on the internet for a long time. Be very careful, keep your own privacy and respect the privacy of others.
- Private messages should be treated with care, as messages are easily leaked and shared publicly.
- Don't disclose any proprietary, private, secure or confidential information relating to our company's personnel, clients, partners or suppliers.
- Don't cite others' opinions unless this person/organisation approves it. Don't use photos or logos unless people or organisations approve it.

Data protection.

In compliance with data protection laws, our company requires that we only store and use an individual's personal data in the way they intended when they provided it to us. In every case, we ask: Why are we holding onto this data, and are we allowed to keep / use it? The following provides further detail with regards to implementation of data protection.

Ethical standards for data collection.

Data collection is an important part of our offering as a company, and we have set high ethical standards for its collection. We employ three basic principles to data collection, whether institutional or individual: fairness, lawfulness and proportionality. We ensure that beneficiaries and stakeholders participating in activities that aim to collect quantitative or qualitative data:

- Are provided with a clear explanation on what type of information we are collecting, who is collecting it and the purpose that information will serve;
- Are notified if whether their data will be shared with other parties; and
- Consent to provide information either written or oral.

We ensure that the data we collect is confidential and transferred only to our clients under the terms and conditions of our contracts. Finally, we ensure that we are only collecting data and information that is necessary to fulfill the terms of our contracts. All participants are notified of these principles so that they can make informed decisions on if, how and what type of information they are willing to disclose.

Where data is being collected from vulnerable beneficiaries in disadvantaged communities, in particular women who have been abused, this presents intricate challenges to building ethical and effective data collection strategies. In these cases, our approach is founded on the bedrock of Ellsberg and Heise's 2005 Researching Violence against Women: A Practical Guide for Researchers and Activists (itself based on WHO's 2001 guidelines), with a particular focus on ensuring that participation in the baseline and evaluation activities does not cause further harm or trauma. We build on this bedrock by integrating protocols (established in advance with local partners) for informing participants about, and referring them to, sources of further assistance, where specific indicators of trauma, violence or a need for social assistance are identified. We ensure that the consultants conducting fieldwork are trained and skilled in providing suitable support to program participants, including sensitivity toward participant's choices and decisions regarding both participation in the program and access to any assistance offered.

Records retention.

All records relating to our business transactions - including compliance, contracts, financial, human resources, information and communications, operations, procurement, risk management, safety and security, client deliverables and other critical records - are created, maintained, and preserved in a complete and accurate manner. They are readily accessible when required and protected from damage or unauthorized access and use. Records must be authentic and not altered in an unauthorized manner.

Records are retained until the specified period of retention has expired, pursuant to the contract to which they relate and the jurisdiction in which they are retained. Where client requirements are different from the local laws on records retention, we comply with the stricter requirement.

Confidential data.

Use of confidential data.

Staff must:

- Be advised of any confidential data they have been granted access to. Such data must be marked or otherwise designated "confidential."
- Only access confidential data to perform his/her job function.
- Not seek personal benefit, or assist others in seeking personal benefit, from the use of confidential information.
- Protect any confidential information to which they have been granted access and not reveal, release, share, email, exhibit, display, distribute, or discuss the information unless necessary to do his or her job or the action is approved by his or her supervisor.
- Report any suspected misuse or unauthorised disclosure of confidential information immediately to his or her line manager or the company's Executive Director.

If confidential information is shared with third parties, such as contractors or vendors, a confidential information or non-disclosure agreement must govern the third parties' use of confidential information. The third party must also be informed how the data is used, secured, and, destroyed.

Treatment of confidential data.

- **Storage** - Confidential information must be removed from desks, computer screens, and common areas unless it is currently in use. Confidential information is stored under lock and key (or keycard/keypad/biometrics), with the key, keycard or code secured.
- **Transmission** - Great care must be taken when transmitting confidential data, to ensure it is only being shared between those authorized to view it, and will not be shared further. Confidential data must not be left on voicemail systems, or otherwise recorded.
- **Destruction** - Confidential data must be destroyed in a manner that makes recovery of the information impossible. The following guidelines apply:
  - Paper/documents: shredding is required.
  - Storage media (CD's, DVD's): physical destruction is required.
  - Hard drives/systems/mobile storage media: physical destruction is required. If physical destruction is not possible, the IT Director must be notified.

Examples of confidential data.

The following list is not intended to be exhaustive but provides guidelines on what type of information is typically considered confidential. Confidential data can include:

- Employee or customer social security numbers or personal information,
- Medical and healthcare information,
- Electronic Protected Health Information (EPHI),
- Customer data,
- Company financial data,
- Sales forecasts,
- Product and/or service plans, details and schematics,
- Network diagrams and security configurations,
- Communications about corporate legal matters,
- Passwords,
- Bank account information and routing numbers,
- Payroll information,
- Credit card information,
- Any confidential data held for a third party.

Risk management.

Good risk management should ensure that an organization makes effective use of a risk framework that has a series of well-defined steps. The aim is to support better decision making through a good understanding of risks and their likely impact.

Our company’s approach to risk management is that of a continuous and developing process, methodically addressing all risks surrounding our activities past, present and future. To this end, our company maintains a risk matrix, which records risks present in our work and the treatment strategy for each, and ensures these risks are reviewed systematically and regularly.

Due diligence.

Due diligence refers to actions taken to identify and evaluate risks associated with a business transaction, and provide inputs to the decision on whether to proceed with a particular business transaction. Due diligence helps to prevent potentially harmful business relationships.

When undertaking due diligence for new consultants or subcontractors, our company conducts formal and informal reference reports, and based on the outcome of this, a decision is made whether or not to proceed with contracting. As part of the contracting process, the consultant/subcontractor is required to sign a certification, declaring that they:

- Have read and understand the Company Code of Conduct.
- Have never been investigated for, charged with, convicted or otherwise implicated in criminal, corrupt, unethical, or unlawful conduct.
- Agree not to engage in any activity, practice or conduct that conflicts with or appears to conflict with the interests of our company, and will notify the company of any situation involving an actual or potential conflict of interest which may arise in the course of performance by the consultant of any obligation pursuant to their agreement.
- Are not linked, directly or indirectly, to organisations or individuals associated with terrorism, and that if found to be, understand their contract at no cost to our company will be terminated immediately.

Should the consultant or subcontractor choose not to sign the certification then our company will not proceed with executing the contract.