



IDG Group DMCC

1405 JBC 5, Cluster W, Jumeriah Lakes Towers, PO Box 50784, Dubai, UAE

CODE OF CONDUCT POLICY

APRIL 2021

VERSION 5

VERSION CONTROL






VERSION	ISSUED	AUTHOR	AUTHORISED FOR RELEASE
1	AUG 16	G WINTER	
2	AUG 17	G WINTER	
3	SEP 17	G WINTER	
4	JAN 20	G WINTER	
5	APR 21	G WADE	



TABLE OF CONTENTS

TABLE OF CONTENTS	1
CODE OF CONDUCT POLICY	1
1. Scope	2
2. IDG's Ethical Principles	2
3. Standards of Conduct and Discipline	3
3.1 Dress and Bearing	3
3.2. Useful Do's and Don'ts	3
4. Code of Conduct	4
5. Safety	5
6. Security	6
7. Confidentiality and Information Security	6
7.1. Social Media and Networking	7

CODE OF CONDUCT POLICY

1. Scope

The following Policy sets out the standards expected by the Company and the Chief Executive Officer (CEO) of all IDG personnel. The Policy is an extract of the Employee Handbook which is provided to all personnel on joining the company but addresses the standards of ethical and good behaviour expected.

The Code of Conduct Policy is based on a number of documents that staff may find useful to understand – you may prefer to ask your line manager if you are interested. These documents are:

- The International Code of Conduct (ICoC) - <https://icoca.ch>
- UN Global Compact (UNGC) - <http://www.unglobalcompact.org.uk>
- The Voluntary Principles for Security and Human rights (VPSHR) - <http://www.voluntaryprinciples.org>
- The Foreign and Corrupt practices Act (FCPA) (USA) - <https://www.justice.gov/criminal-fraud/foreign-corrupt-practices-act>
- The Bribery Act (UK) - <https://www.legislation.gov.uk/ukpga/2010/23/contents>

2. IDG's Ethical Principles

IDG prides itself on its ethical standards. To achieve this requires every one of IDG's staff, and the sub-contractors we work with to adhere to the highest ethical standards. Our ethical standards are based on the respect and adherence to fundamental and universal human rights of all. These principles are:

- Right to life
- Right to freedom of movement
- Freedom of expression and peaceful assembly
- IDG demands zero tolerance of:
 - Slavery, indentured and forced labour, child labour and human trafficking
 - Harassment and bullying
 - Sexual exploitation and abuse
 - Corruption



-
- Discrimination (equality, diversity and inclusion)

All these principles are defined in IDG's Policies which are available to all staff at all levels and are included as part of your employee information packs as well as held online on the IDG Security website.

3. Standards of Conduct and Discipline

You must know, understand and follow IDG's ethical principles (above).

You are expected to carry out instructions in accordance with your employment contract.

You should not undertake any activity which is not covered by the company's insurance policy. You should know relevant local laws and the rules of the Company's client.

You must ensure you know and understand the operational orders, guard orders, fire orders, stand-to and contingency plans, Standard Operating Procedures (SOPs), Rules for the Use of Force (RUF) and other orders and instructions relevant to your place of work.

You should tell, by the quickest possible means, your Supervisor, Project Manager or Country Manager if you have an administrative, welfare or operational problem, giving full and accurate details.

3.1 Dress and Bearing

Uniform and dress can project a positive image of the organisation and are key to encouraging professional and responsible behaviour by IDG personnel. Personal appearance and bearing can have a huge impact on how you as an individual, and by extension the Company, are perceived. Eyes are always on us, whether it be the client or a potential enemy and we must always look well-turned-out and alert.

If you are issued IDG clothing / uniform you must wear it, always presenting a clean, professional appearance. You are expected to be well-groomed and wear clean clothing / uniform, free of holes, tears, or other signs of wear. This is particularly the case for IDG Guards and Supervisors, as per your contractual requirements.

If you are in a management role you must be conscious of setting an example to the teams on the ground, as well as looking smart, professional and impressive to the client. This means smart office wear suitable for the climate, and always excludes items such as shorts and flip flops.

Representing the organisation and looking smart is a part of the image of professionalism that IDG projects, both internally and externally.

3.2. Useful Do's and Don'ts

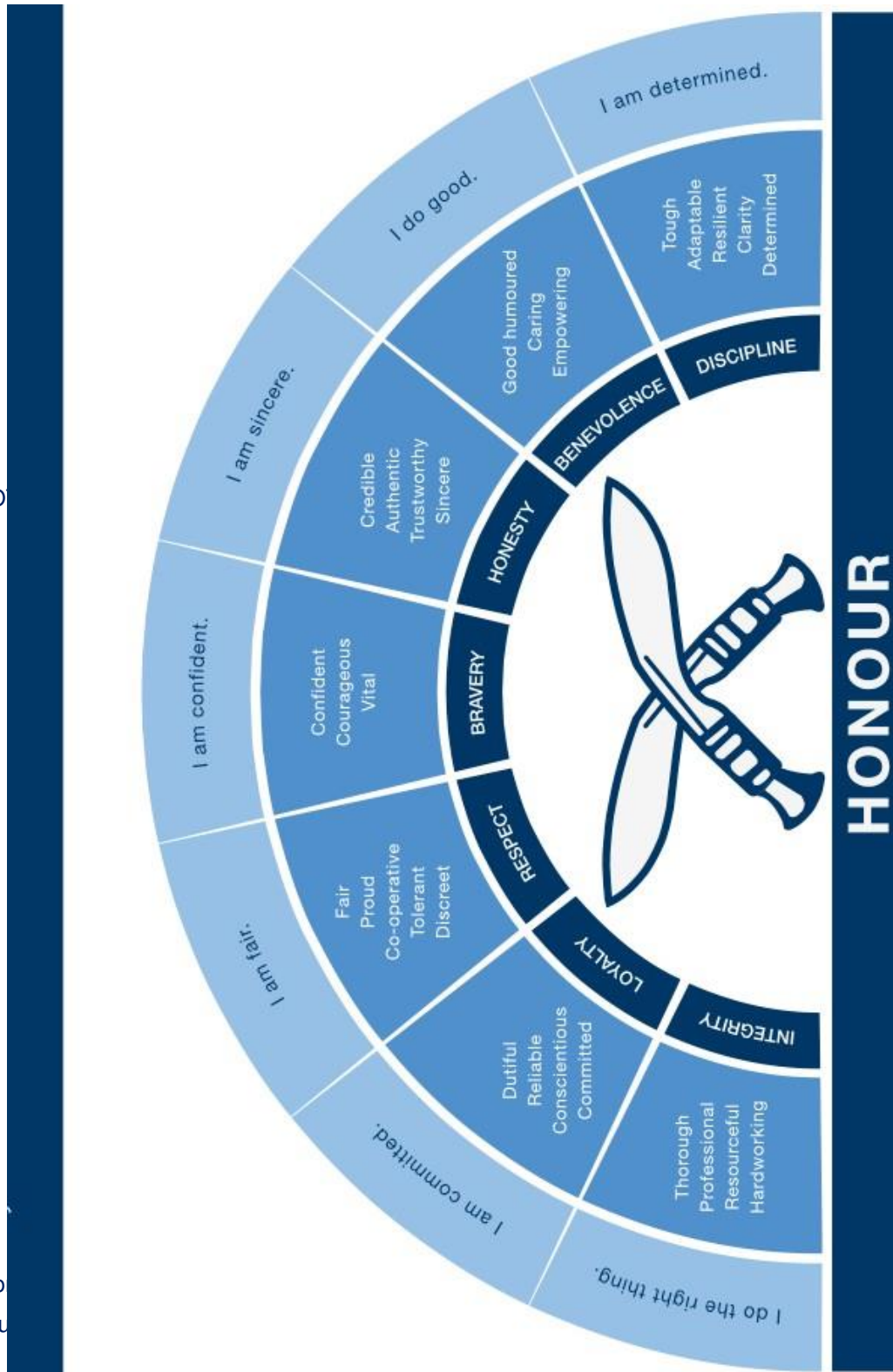
DO

- Learn as much of the local language as you can
- Improve your English
- Be firm and friendly

DO NOT

4.

The Co
the valu



sents



5. Safety

Security duty can be repetitive and may lead to boredom. Lack of alertness is the enemy of security. A smart, alert, professional bearing is the first weapon in your armoury and will send most enemy elsewhere to find an easier target.

Be aware of the climate and water in the country in which you will be working and make sure you have clothing that is suitable for all seasons if necessary. Good personal hygiene, maintaining fitness, keeping healthy and consuming plenty of water is vital to operational efficiency.



Many countries have a land mine threat, so always watch where you are walking and placing your hands.

Avoid washing and swimming in rivers if possible. Rivers may have strong currents or contain disease or dangerous animals. If you must visit and use a river, go with at least one other person.

It is recommended that mail is posted by reliable means or passed to IDG management or the PM so that it can be posted from a reliable centre.

It is best to not leave valuable personal effects in your accommodation and it is also not practical to carry everything with you. If you are in possession of a large amount of money or gold (not likely) and you feel that security is not good, then it is advisable to leave it with IDG management or the Project Manager. Exercise care over the security of all your possessions.

6. Security

Security IS our business, and you MUST think “Security” at ALL times. Always be alert, even when off duty. Be always suspicious and curious. Never take anything at ‘face’ value. Remember the Nepali proverb: **“Mukhma ‘Ram Ram’, bhaguli ma chhuri cham”!** Always question and check.

7. Confidentiality and Information Security

Operational and Commercial security require that you observe care when using all communications systems. Failures of operational security can cost you your life. Commercial security lapses can cost you your job.

Any written or verbal information about the company and the company’s operations. This includes anything stored, transmitted, or viewable on telephone conversations and messages, emails, electronics message services, computer stored information and USB memory sticks, documents, files, and notes.

Be extremely careful what you say on mobile phones. Always assume that someone else is listening. The internet and all email communications are monitored by governments, some of whom may be friendly to terrorists.

- Do be careful what you write in emails and electronic messages
- Do be wary of emails from unknown sources inviting you to reply, give information or even to open attachments
- Do not action emails from unknown sources but delete them and report it to your superior
- Do not forward emails within the Company from unknown sources as you could be forwarding viruses or spyware



-
- Do not send emails inviting Company staff to join networks or chat groups without first warning people that you will be inviting them

 - Do ignore and delete invitations to join groups received from anyone unless that person has warned you in advance of the invitation and you know it is genuine and really from that person.

The IDG Data Protection and Information Management Policies must be read and adhered to.

7.1. Social Media and Networking

This policy provides guidance for your use of social media and networking technologies / service. This includes blogs, wikis, micro-blogs, message boards, chat rooms, electronic newsletters, online forums, social networking sites, and other sites and services that allow people to share information with others.

IDG views social media and networking services as a normal and important element of its employees' social and domestic lives. It is IDG's stance that these tools are considered suitable for personal purposes but not for professional use within IDG: they are subject to too great a risk of an operational security breach. The only exemption to this is the use of business sites such as LinkedIn (where individuals state IDG Security as their employer), used in particular by the IDG Senior Management Team for the promulgation of messages and the recruitment of new personnel.

IDG is proud of the quality of our work, and immensely proud of our employees: but this is not something we boast about, advertise, or tell people. IDG operates in difficult and dangerous environments, providing security services to its clients, and we are therefore expected to provide the very highest standards of security. This includes reducing the chances of any breach of operational security. IDG therefore requires strict social media guidelines to be applied.

Two basic rules apply:

1. Don't help the enemy by providing them with any information, however trivial it may seem.

2. Anonymity is your best defence, and the best defence for your colleagues. Don't make yourself a target.

You are required to reduce your personal 'online presence' to the smallest extent possible when it comes to your professional role within IDG. You are not to publish any written or pictorial information on any aspect of IDG, its operations, or those of its clients. This means photographs, videos, diagrams, comments, updates, etc, no matter how trivial or innocent they may seem.

If you are using social media privately and see an error, criticism or allegation about IDG, do not be tempted to respond, even if that this might be corrected through a quick response: in these cases, you are to alert the Country Manager who will determine what action, if any, is appropriate.

