Code of Conduct

(Amendment – 1)

Valid with effect from 01st April 2015

- **SCOPE**

The scope of this document is

- to assess the impartiality threat risk for the IGEP Trust and its employees.
- To have a Confidentiality Code of Conduct for Staff

- **REFERENCES**

.1 Internal

- IGEP Trust Ethical Code of Conduct

.2 External

- ISO/IEC 17000:2004 Conformity assessment – Vocabulary and general principles;
- ISO/IEC 17065:2012: Conformity assessment – requirements for bodies certifying products, processes and services.
- ISO/IEC 17020:2012 Conformity assessment – Requirements for operation of various types of bodies performing inspections
- ISO/IEC 17021:2011 Conformity assessment – Requirements for bodies providing audit and certification of management systems
- ISO/IEC 17024:2012 Conformity assessment – General requirements for bodies operating certification of persons
- ILO (International Labour Organisation) – Guidelines on Occupational Health and Safety Management Systems
- Information Technology Act, 2000 (IT Act)
- Protection of Human Rights Act, 1993.
- Child & Adolescent Labour (Prohibition & Regulation) Act, 1986- Having information of child labour must report to the 1098 Child line-Helpline /Police/Child Welfare Committee (CWC) or Labour Officer
- Juvenile Justice (Care & Protection of Children) Act, 2015 : Having information on any kind of exploitation of the child report to the 1098 Childline-Helpline /Police/Child Welfare Committee (CWC)
- Protection of Children from Sexual Offences (POCSO) Act, 2012- Mandatory reporting to the Police : As per Section 21(1) of the POCSO Act, 2012 requires a person having information on any kind of sexual abuse of a child , the person with knowledge must inform the police. It applies to everyone including parents, doctors and school personnel. Failure to report a suspicion of child abuse is an offence under the Act
- The Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013- It is a legislative act in India that seeks to protect women from sexual harassment at their place of work.
- Right to Privacy: Employees and management to respect the privacy of others in the office set-up. These concepts of privacy flagged under different international instruments are as follows: Article 12 of Universal Declaration of Human Rights (1948) states that “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence nor to attack upon his honour and reputation. Everyone has the right to protection of the law against such interference or attacks.” Article 8 of European Convention on Human Rights states “Everyone has the right to respect for his private and family life, his home and his correspondence.

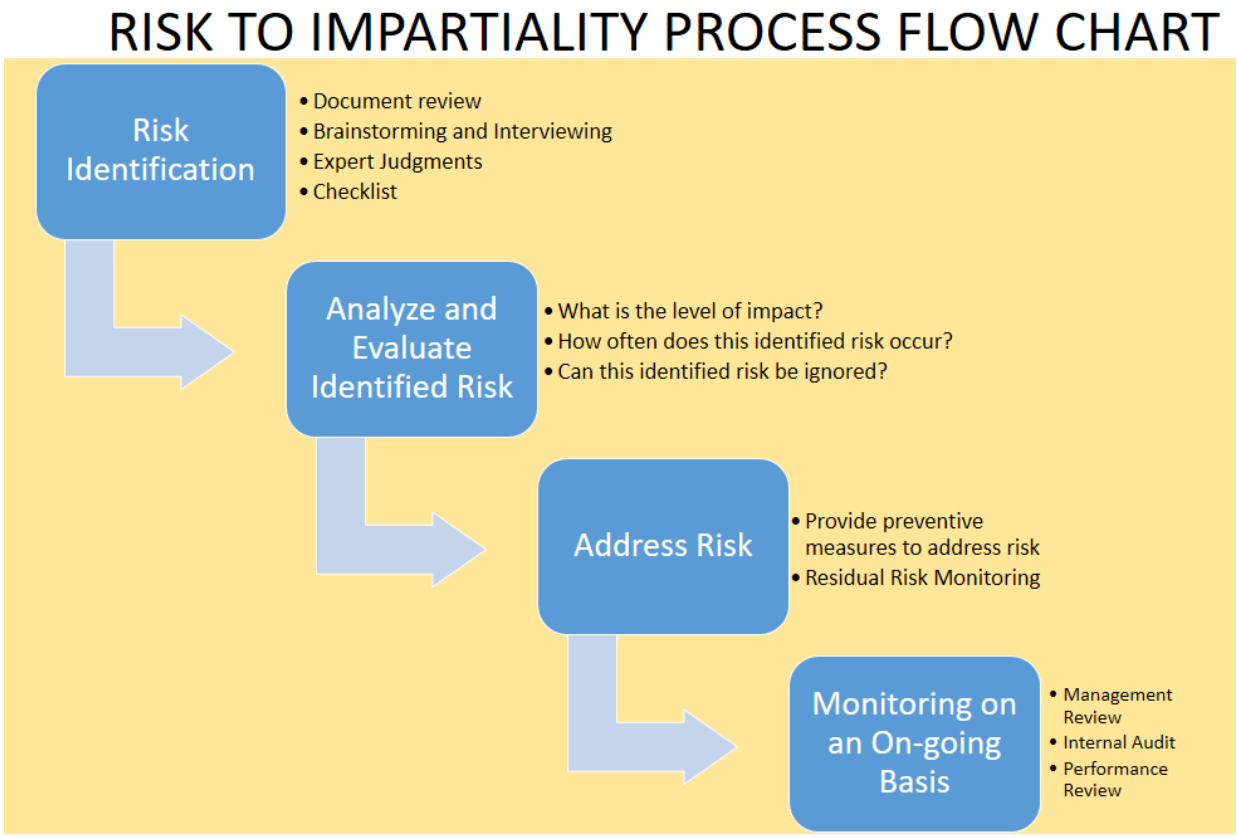

Diagram describing flow chart 'How to Identify and Address the Risk to Impartiality'

➢ **IMPARTIALITYSTRUCTURE**

The Impartiality Risk Management Report is the tool to identify, describe and measure the inherent and residual impartiality risks.

Impartiality consists of:

TP ***Principal Text*** (Impartiality–TP): it defines impartiality threats, sensitive activities and the relationships between the companies

AD ***Addendum*** (Impartiality–AD): it defines in detail the impartiality risks within the company, as applicable

DB ***Impartiality***: ***Risk Management Database*** (Impartiality-DB): it contains the evaluation of inherent risks, control measures and residual risks.

➢ **IMPARTIALITY UPDATE PROCESS**

Impartiality is updated through *a continuous revision process* involving:

("IGEP Trust"): it defines:

- Impartiality threats;
- Subsidiaries and their relevant activities;
- Sensitive activities;
- Risk Management process

TP is updated in the following cases:

- Acquisition/Disposal of a subsidiary;

- Group's re-organization.

Sub-Contractors: it develops and updates its AD and defines:

- Applicable sensitive activities;
- For each applicable sensitive activity, the relevant modalities, arising from services and relationships;
- For each modality, calculation of the inherent risk, control measures and residual risk.

AD is updated in the following cases:

- Re-organization;
- New services;
- New relations;
- New accreditations or authorisations,

Any update to the TP is sent to the Board for approval.

Any update to the AD is approved by the Safeguard Impartiality Board (SIB) and sent to IGEP Trust Board for information.

The sub-contractors may request the holding to add new sensitive activities or to review the existing ones. Table 1 summarizes the revision process and the relevant responsibilities:

Table 1

Function	***Impartiality part***	***Responsibility***
Corporate Compliance & Risk Management	Principal Text (Impartiality-TP)	Preparation, update and submission to Board for approval
Corporate Compliance Board (CCB)	Principal Text (Impartiality-TP)	Approval and publication on the IGEP Trust Portal
Safeguard Impartiality Board (SIB)	Addendum (Impartiality-AD)	Preparation, update, approval, submission to Board for information and publication on the IGEP Trust Portal
Corporate Risk Management	Addendum (Impartiality-DB)	Management and update

➢ RISK MANAGEMENT PROCESS

Enterprise Risk Management Process describes the process adopted by IGEP TRUST for managing enterprise risks in accordance to applicable regulations and/or procedures.

➢ THREAT AND SENSITIVITY ACTIVITIES

A *sensitive activity* is the event (area/process/situation) where a threat to impartiality (conflict of interest) may arise.

Threats to impartiality include the following categories:

1. **Self-interest threats**: threats that arise from a person or body acting in their own interest. A concern related to certification, as a threat to impartiality, is financial self-interest;
2. **Self-review threats**: threats that arise from a person or body reviewing the work done by themselves. Auditing the management systems of a client to whom the certification body provided management systems consultancy would be a self-review threat;

3. **Familiarity (or trust) threats**: threats that arise from a person or body being too familiar with or trusting another person instead of seeking audit evidence;

4. **Intimidation threats**: threats that arise from a person or body having a perception of being coerced openly or secretively, such as threats to be replaced or reported to a supervisor.

Impartiality may be affected by the following relationships:

A. Ownership, governance, direction

B. Personnel

C. Contracts, marketing, sales commissions, incentives

D. Services other than third party conformity assessments

E. Shared resources

F. Financial resources

The identified sensitive activities are grouped according to the above-mentioned four categories of threats and six types of relationships (see Table 2).

Table 2

Code	***Threat category***	***Conflict Type***	***Sensitive activity***
1.A.01	Self-interest threat	Ownership, governance, management	A subsidiary (certification body) owns shares in a company certified/inspected by the same subsidiary or by another subsidiary.
1.A.02	Self-interest threat	Ownership, governance, management	The shareholders (individuals) of a subsidiary (certification body) owns shares or have corporate positions in: ▪ companies certified/inspected by the same subsidiary; ▪ consulting companies.
1.A.03	Self-interest threat	Ownership, governance, management	The subsidiary (certification body) owns shares in consulting companies.
1.A.04	Self-interest threat	Ownership, governance, management	The shareholders(legal entities) of a subsidiary (certification body) are consulting companies or companies certified by the same subsidiary or companies engaged in the design, manufacture, supply, installation, purchase, ownership, use or maintenance of the items inspected by the subsidiary.
1.A.05	Self-interest threat	Ownership, governance, management	The shareholders (legal entities) of the subsidiary (certification body) are trade associations.
1.A.06	Self-interest threat	Ownership, governance, management	The shareholders (legal entities) of the subsidiary (certification body) are SOA (Service-oriented architecture).

1.A.07	Self-interest threat	Ownership, governance, management	The subsidiary (inspection body) is linked to a separate legal entity engaged in the design, manufacture, supply, installation, purchase, ownership, use or maintenance of the items inspected by the following: ▪ common ownership, ▪ common ownership appointees on the board or equivalent of the organizations; ▪ directly reporting to the same higher level of management.
1.A.08	Self-interest threat	Ownership, governance, management	The subsidiary (certification/inspection body) entrusts third-party conformity assessment to consulting companies.
1.A.09	Self-interest threat	Ownership, governance, management	Direction and co-ordination of the holding on sub-holdings and their controlled companies
1.A.10	Self-interest threat	Ownership, governance, management	Multiple roles within Operative Companies.
1.B.01	Self-interest threat	Personnel	The technical staff of the subsidiary (certification/inspection body) and/or consultants (non-exclusive personnel): ▪ has / had corporate positions, ▪ has / had different positions (temporary contracts, work-for-hire contracts, etc.), ▪ owns / owned shares, in companies certified or being certified or linked with the scope of the third party assessment.
1.B.02	Self-interest threat	Personnel	The manager of a subsidiary (certification body) assigns a third-party conformity assessment to a family member associated of him
1.B.03	Self-interest threat	Personnel	The technical staff of the subsidiary (certification/inspection body) performing third-party conformity assessment has commercial incentives (to issue certificates, to acquire customers) not associated with qualitative objectives
1.C.01	Self-interest threat	Contracts, marketing, sales commissions, incentives	Consulting activities are promoted/advertised in conjunction with third- party conformity assessment activities (or vice versa).
1.C.02	Self-interest threat	Contracts, marketing, sales commissions, incentives	The subsidiary (certification/inspection body) gives financial support to/sponsors activities carried out by consulting companies (e.g. training courses, conferences, meetings, etc.) or vice-versa consulting companies give financial support to/sponsor activities carried out by the subsidiary (certification/inspection body).
1.C.03	Self-interest threat	Contracts, marketing, sales commissions, incentives	The subsidiary (certification/inspection body) delivers services together with consulting companies (or vice-versa).
1.C.04	Self-interest threat	Contracts, marketing, sales commissions,	The subsidiary (certification body) pays fees to consultants/consulting companies for the acquisition of a

		incentives	certification contract.
1.C.05	Self-interest threat	Contracts, marketing, sales commissions, incentives	Invoicing to the customer done directly by the consulting company or by an agency acting in the name and on behalf of the subsidiary(certification body)
1.C.06	Self-interest threats	Contracts, marketing, sales commissions, incentives	The subsidiary gives discounts (or surcharges) to certain organizations
1.C.07	Self-interest threats	Contracts, marketing, sales commissions, incentives	The subsidiary gives promotional activities (e.g.: free or reduced-cost training courses) to certain organizations.
2.A.01	Self-review threat	Ownership, governance, management	The subsidiary (certification/inspection body) certifies: ▪ the management system of another subsidiary; ▪ the Quality management system of any other certification body.
2.A.02	Self-review threat	Ownership, governance, management	The subsidiary (certification/inspection body) provides: ▪ inspection/audit activities (under accreditation or not); and ▪ conformity assessment services (under accreditation or not) to customers (or on items) for which the subsidiary or another company of the Group carried out consulting activities
2.D.01	Self-review threat	Services other than third party conformity assessments	The subsidiary (certification/inspection body) and its personnel, as well as any part of the same legal entity and entities under its organizational control: ▪ carries out consulting activities; ▪ is engaged in the design, manufacture, supply, installation, purchase, ownership, use or maintenance of the certified product/process and/or inspected item.
2.D.03	Self-review threat	Services other than third party conformity assessments	The subsidiary (certification body) provides: ▪ catalogue training courses at its or customer's premises; ▪ compulsory safety training; ▪ training courses to personnel subject to subsequent certification
2.D.04	Self-review threat	Services other than third party conformity assessments	The subsidiary (certification body) performs: ▪ second and third party audits, in compliance with standards other than those included in the accreditation scope; ▪ other assessment activities that do not provide specific solutions, but gap analysis only; ▪ technical diagnostic tests; ▪ second party audits of certified company's suppliers.
3.B.01	Familiarity threat	Personnel	The subsidiary (certification body) always assigns a third-party conformity assessment to the same auditing team.

3.E.01	Familiarity threat	Shared resources	The subsidiary (certification body) shares offices, branches or personnel with consulting companies.
3.E.02	Familiarity threat	Shared resources	The subsidiary (certification body) and SOA (Service-oriented architecture) have common shareholders.
3.E.03	Familiarity threat	Shared resources	The subsidiary (certification body) participates (as guest or speaker) in services delivered by consulting companies (e.g. training courses, conferences, meetings).
4.A.01	Intimidation threat	Ownership, governance, management	Employees of the subsidiary who in order to achieve their economic and quantitative objectives request unethical behaviours of other employees.
4.B.01	Intimidation threat	Personnel	Employees of the subsidiary who, misusing their position, force anyone to provide, for themselves or others, money/benefits not due.
4.B.02	Intimidation threat	Personnel	Employees of the subsidiary (certification body) who, misusing their position, state or imply that certification/verification/validation would be simpler, easier, faster or less expensive if a specific consultancy company is used.
4.B.03	Intimidation threats	Personnel	Employees/consultants (non-exclusive personnel) of the subsidiary who due to intimidation by the client carry out activities in an inadequate way.
4.B.04	Intimidation threats	Personnel	Employees/consultants (non-exclusive personnel) of the subsidiary who due to late scheduling of activities is forced to operate under pressure.
4.F.01	Intimidation threats	Financial resources.	Subsidiary activities are impaired by the client's economic and financial influence.
4.F.02	Intimidation threats	Financial resources.	A significant amount of the subsidiary's (certification body) turnover comes from clients connected to the same consultancy company.
4.F.03	Intimidation threats	Financial resources.	The subsidiary (certification body) is financed by a certified or a consulting company

Confidentiality Code of Conduct for Staff

In the following context IGEP Trust is referred as 'we' and the employees of IGEP Trust are referred as 'you' or 'your'.

All employees working in/with the IGEP Trust are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the Information Technology Act, 2000 (IT Act).

This means that employees are obliged to keep any personal identifiable information strictly confidential. It should be noted that employees also come into contact with non-person identifiable information which should also be treated with the same degree of care e.g. business "in confidence" information.

This means that we take every measure to make sure that all clients and staff information is processed fairly, lawfully and with as much transparency as possible so that the public and staff:

1. Understand the reasons for processing personal information
2. Give their consent for disclosure and use of their personal information
3. Have complete trust in the way the IGEP Trust handles its information
4. Understand their rights to access information held about them

The principle behind this Code of Conduct is that no employee shall breach their legal duty of confidentiality, allow others to do so, or attempt to breach any of the IGEP Trust's security systems or controls in order to do so.

This code of conduct outlines your personal responsibilities concerning security and confidentiality of information relating to clients, staff and the organisation. This document has been produced to protect staff by making them aware of correct procedures so that they do not inadvertently breach any of the requirements placed upon them.

All employees of the IGEP Trust are expected to act and behave in accordance with the company values of safety and respect in relation to any company related staff or client information that they may encounter during the course of their duties.

During your employment with the IGEP Trust you may acquire or have access to confidential information which must not be disclosed to any other person unless it is required to be disclosed in pursuit of your duties or the individual concerned has given their specific permission or consent. This condition applies during your relationship with the IGEP Trust and also remains after you have left the organisation.

What are the Different Types of Confidential Information

- Client Records
- Staff Records
- Recruitment and selection
- Telephone enquiries about clients /staff
- Electronic databases
- Methods of communication
- Use of fax machines
- Hand written notes containing client information or staff information
- Video and sound files containing client information or staff information

What is Personal Identifiable Information

Anything that contains the means to identify a living person. If there should be any doubt as to what information may be disclosed clarification must be sought from your line manager.

What are Your Responsibilities

Under the terms of your signed contract of employment you must, at all times, be aware of the importance of maintaining confidentiality and security of information gained by you during the course of your duties. This will, in many cases, include access to personal information relating to service users. You must treat all information, whether corporate, staff or client information, in a discreet and confidential manner in accordance with the provisions of the Information Technology Act, 2000 and organisational policy.

What Does the Information Technology Act, 2000 do

The Information Technology Act, 2000 regulates the use of computerised information and paper records and images of identifiable individuals / companies (clients and staff).

Information Technology Act and use of E-Mails

The use of emails is also covered by the act therefore caution should be taken in sending and forwarding emails within the IGEP Trust and extreme caution taken in sending emails outside of the company. The IGEP Trust is registered in accordance with this legislation. If you are found to have made an unauthorised disclosure you may face legal action.

What Must you be Aware of with Confidentiality

You must at all times be aware of the importance of maintaining confidentiality of information gained during the course of your duties. All information must be treated in a discreet and confidential manner, and in accordance with the IGEP Trust's Confidentiality Code of Conduct, the Information Technology Act, 2000 and the Data Protection and confidentiality policies which are available on the internet. Your duty of confidentiality arises out of the common law of confidentiality, professional and statutory obligations.

What would be considered as a Breach of confidence

Inappropriate use of audit or staff records or abuse of computer systems may lead to disciplinary action, bring into question professional registration and possibly result in legal proceedings. All workers must therefore ensure that they are aware of the requirements and standard of required behaviour (see Confidentiality and Information Technology Act and your contract of employment details).

What you Can/Cannot do

Your attention is drawn, in particular, to the following:

- Personal data protected under legislation must not be disclosed either verbally or in writing to unauthorised persons. It is particularly important that you ensure the authenticity of telephone enquiries.
- Written records, computer records and correspondence pertaining to any aspect of the IGEP Trust's activities must be kept securely at all times and be inaccessible to members of the public.
- Paper based person-identifiable information or confidential information requiring disposal should be done so in a confidential and secure manner where ever possible by the use of "Confidential Waste" bins.
- You must ensure that all computer systems that you use are protected from inappropriate access within your direct area of practice.
- If it is necessary to share information in order to effectively carry out your work, you must ensure that as far as is reasonable this information will be exchanged on a strictly 'need to know' basis, using the minimum that is required and be used only for the purpose for which the information was given.
- Conversations relating to confidential matters affecting clients/staff should not take place in situations where they may be overheard, e.g. in corridors, reception areas, lifts and cloakrooms. Given the highly confidential nature of the work you may undertake, you should understand that telephone conversations, in particular, should be conducted in a confidential manner.
- Any breach of the Confidentiality Code of Conduct and /or the IT Acceptable Use or Data Protection Policy may be regarded as misconduct and may be subject to disciplinary action, up to and including dismissal. Should you breach this clause after your employment has ended the organisation may take legal action against you.
- The same provisions apply if you are working off-site or at home.
- If you require an explanation concerning the interpretation or the relevance of this Code of Conduct you should seek advice from your manager.
- Any concerns regarding confidentiality issues within an area should be raised with the manager in accordance with the relevant IGEP Trust policy.
- You will not at any time during your employment (except as so far as is necessary in the course of your employment) or afterwards, disclose to any person any information as to the business, dealings, practice, accounts, finances, trading, software, know-how, affairs of the IGEP Trust or any of the IGEP Trust's clients or prospective clients, distributors, firms or companies otherwise connected with the IGEP Trust.
- Employees who are asked to access information relating to colleagues, friends or relatives need to declare their relationship to their manager, who will decide if the task could be carried out by another staff member.
- All information held about the IGEP Trust or in connection with the IGEP Trust, and any of the above, is to be regarded as confidential. All notes, memoranda, records and other documents of the employer which may be in your possession are and shall remain the property of the employer and shall be handed over by you to the employer from time to time on demand and, in any event, upon termination of your employment.
- Any requests for information from the Media (newspapers, TV companies etc.) should always be referred to the IGEP Trust Communication team.

What if people ask us to stop sharing/disclosing their information

Any Individual can at any time make a decision to restrict or prevent disclosure or sharing of their personal information. Any such decisions must be respected by staff and noted within the client's records.

Updating and Training

It is a mandatory requirement that all staff and others dealing with personal identifiable information keep up to date with IG training and developments.

IMPLEMENTATION

The Amendment 1 in Code of Conduct was approved by the Operations Council and by the Board of Directors of IGEP TRUST. The Professional Conduct Committee of the Board of Directors receives regular reports on breaches and oversees its implementation.

The Code takes effect from April 2015.

IGEP TRUST affiliates are authorized to adopt more detailed or restrictive policies in areas covered by this Code, with the prior written approval of the IGEP TRUST Chief Compliance Officer.

CONTACT INFORMATION

Address: The Peach Tree, 2nd Floor, Block – C, Sushant Lok, Phase – 1, Sector 43, Gurgaon-122002, Haryana, India
Internet: www.igeptrust.in
Email: igeptrust@igep.org
Phone: +91 (0)124 4048273 / 77
Fax: +91 (0)124 4048275

A special thank you to all employees and stakeholders for their constructive contribution to our Code of Conduct.