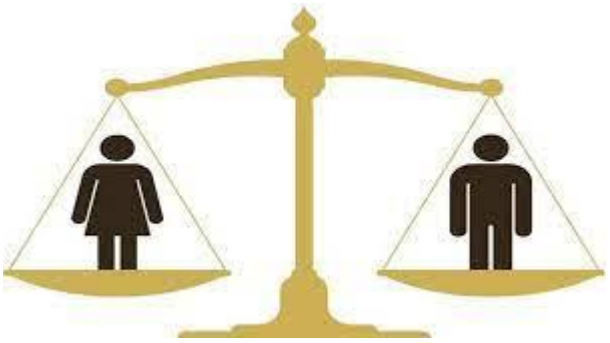
INTEGRITY, DUE DILIGENCE & SAFE GUARDING POLICY OF SACMID



Supported by : Free Press Unlimited under PRIMED Project

Policy Development Team:

Syed Kamrul Hasan (SACMID)

Afia Sultana(SACMID)

Md.Saimum Reza (External Consultant)

Reviewed by: Andre Oostrom (FPU)

April 2022

TABLE OF CONTENTS

Integrity, Due Diligence & Safe Guarding Policy of SACMID

PREFACE

There is a growing awareness within organizations, government and the business community that the mission, strategy and results achieved are intrinsically linked to the relationships among stakeholders and to the integrity, due diligence and safeguarding of an organization. This also applies to the South Asian Center for Media in Development (SACMID). SACMID defines an ethical organization that acts in accordance with justice. This means that the organization does right by the people and organizations with whom and for whom it works. An ethical organization is an organization that is prepared to do right by all its stakeholders. The primary responsibility for this policy lies with the Executive Head of SACMID. However, the responsibility also lies with every employee, staff, director, trustee, board member, advisor, associates, clients, agents, service receivers, partners, respondents, beneficiaries, affiliates and any other stakeholders of SACMID (hereinafter mentioned as Person or Legal Entity concerned to SACMID).

SCOPE

This policy shall be known as **Integrity, Due diligence & Safe Guarding Policy**, hereinafter mentioned as the **Policy**.

The Policy applies to anyone who is represented by SACMID in any way and/or is connected to SACMID through a contract or conduct with any of the SACMID's operational activities. This includes Person or Legal Entity concerned to SACMID .

The whole Policy is divided into four parts. First, three parts discuss three different Codes and the fourth part contains details on reporting and complaint procedures as follows:

PART 1: The Code of Conduct
focuses on interpersonal violations (behaviors) such as discrimination, intimidation, humiliation, bullying, and sexual harassment; behaviors that SACMID does not tolerate.

PART 2: The Anti-Fraud & Corruption Policy
describes what SACMID understands as fraud and corruption, including unacceptable acts such as an abuse of power, conflicts of interest, leaks of confidential information, culpable negligence etc., as well as financial violations such as fraud, theft, forgery and abuse.

PART 3: The Whistle Blowing Policy
SACMID has a system for reporting such violations.This reporting system is openly available to anyone who wants to report or file a complaint. This includes a procedure for whistle-blowers. If an employee does not have confidence in the management of SACMID, s/he can make her/his report to an external whistle-blowing contact.

PART 4. Report & Complaint Procedure

Describes the detailed reporting and complaint management procedures to deal with any complaint in relation to the abovementioned Code of Conduct, the Anti-Fraud & Corruption Policy and the Whistle Blowing Policy.

DEFINITIONS

- **Feedback;** any comment or remark or analysis or assessment or observation or findings or remarks on any operation, conduct, service, commencements, implementation and initiative by SACMID.

- **Complaint;** If a Person or Legal Entity concerned to SACMID acknowledges or claims to have suffered or may suffer loss or damages or received/faced or may receive/face injustices due to a breach of a duty imposed on the concerned person(s), subject to conditions or restrictions or reservations stipulated in any policy or guidelines or framework or procedures by SCAMID. The complaint shall be served and processed duly according to the procedures described under this Policy.

- **Report;** Reporting any information, concerns or substantial suspicions of breaches of this Policy or any other policies, procedures or codes of SACMID.

- **Appeal;** Appeal against any decision or remarks or analysis of Complaint filed or processed under this Policy.

- **Team;** Feedback Management and Complaint Redressal Team, formed by SACMID under this Policy, for proper, speedy and smooth disposal of feedback or complaints.

- **Appellate Team;** Team to assess and deal with the appeal against decisions on any complaint filed to SACMID. SACMID will form such a team, under this Policy.

- **Whisleblowing;** A confidential disclosure by an individual, or group of people, who is a Person or Legal Entity concerned to SACMID, encountered in the workplace relating to perceived wrongdoing or malpractices and threaten the public interest; subject to compliance with the **Part 3: The Whistle Blowing Policy** of this Policy

- **Fraud, Corruption & Forgery:** The definitions mentioned in the **PART 2: The Anti-Fraud & Corruption Policy** under this Policy

- **Pseudonymization:** the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information. For example- the information that can point to the identity of a person or data subject is replaced by “pseudonyms” or identifiers.

- **Data:** data means any categorized or non-categorized information about an incident or fact or issue or matter or procedure or initiative.

- **Personal data:** data that reveals the identity of any natural or legal person, or data that makes the identity of any natural or legal person revealing.

PART 1: THE CODE OF CONDUCT

1A: SACMID Principles:

- **Compliance with laws;** All business and other activities of SACMID shall be carried out in compliance with all applicable laws, and principles of the country. Each Person or Legal Entity concerned to SACMID is expected to comply with the requirements of those laws and regulations that apply to SACMID's operations and to his/her/its job responsibilities or relation to SACMID.

- **Openness;** SACMID promotes openness and transparency, as well as continuous dialogue with Person or Legal Entity concerned to SACMID, including government agencies, academia, civil society, corporate sector, local communities, industry and the media. SACMID strives to be honest and accurate when communicating with Person or Legal Entity concerned to SACMID, and they shall make their statements in accordance with these principles.

- **Respect for human and labor rights;** SACMID supports and respects the protection of human rights as defined in the Universal Declaration on Human Rights and in other human rights principles enshrined in the Covenants or Treaties or Conventions of the United Nations. No employee shall be allowed to take any action that violates these human rights principles, either directly or indirectly, in any circumstances. SACMID supports basic labor rights as defined by the International Labor Organization (ILO). In this respect, these rights are restricted by local law and SACMID endeavors to offer Person or Legal Entity concerned to SACMID alternative means to present their views. SACMID does not accept any form of forced labor, or the use of child labor. Therefore, every action, decision, operation, procedure, initiative and commencements of SACMID shall follow the rights-based approach.

- **Fair employment practices;** SACMID promotes freedom from discrimination based on race, ethnic or national origin, color, gender, family status, sexual orientation, creed, disability, age or political beliefs, or other characteristics protected by law. SACMID fosters equal opportunity and gender balance. Person or Legal Entity concerned to SACMID are selected and treated on the basis of their abilities and merits. SACMID shall not accept any form of discrimination, harassment, racism, nepotism, prejudice or bullying from Person or Legal Entity concerned to SACMID.

- **Occupational health and safety;** SACMID endeavors to create hazard-free workplaces for Person or Legal Entity concerned to SACMID by applying high standards of occupational health and safety. SACMID strives to assure the safety of its services and solutions through its world-class service and solution development processes. Each Person or Legal Entity concerned to SACMID is responsible for complying with the safety instructions developed by SACMID, for using personal protection equipment when required, and for reporting on any shortcomings regarding safety instructions or protection measures. Higher threshold of safety measures shall be maintained by all Person or Legal Entity concerned to SACMID in case of pandemic, natural disaster or war or any other emergency situation as stated in Safety Instructions developed by SACMID.

- **Conflicts of interest;** SACMID expects full loyalty from Person or Legal Entity concerned to SACMID. They must avoid situations where their personal interests may conflict with the objectives of SACMID. This means, for instance, that Person or Legal Entity concerned to

SACMID are not allowed to accept gifts or entertainment from a stakeholder, holding profitable positions in conflict with the employee's position in SACMID, being a member of political party, using any assets of SACMID for personal benefit and any other situation defined by the SACMID in due course of business.

- **Anti-corruption;** No Person or Legal Entity concerned to SACMID may, directly or indirectly, shall promise, offer, pay, solicit, or accept bribes or kickbacks of any kind, including money, benefits, services or anything of value. Such payments and favors shall be considered bribery, which violates local legislation and internationally recognized principles for combating corruption and bribery, subject to the proper and transparent investigation conducted by SACMID .For details, Person or Legal Entity concerned to SACMID shall follow SACMID's Anti-Fraud & Corruption Policy.

- **Environment;** SACMID's target is to develop and produce environmentally advanced solutions and services for Person or Legal Entity concerned to SACMID that fulfil essential requirements, such as low emissions and high efficiency. Efforts are made to achieve sustainable development, as stated in United Nations Sustainable Development Goals (SDGs), by means of eco-friendly raw material selection, processes, products, wastes, and emissions through the use of the latest technological advances. Each Person or Legal Entity concerned to SACMID shall comply with the policies and instructions regarding internationally recognized environmental protection mechanism and any such policies developed by SACMID.

- **Relationship with authorities and local communities;** SACMID maintains constructive cooperation with authorities and regulatory bodies, at both local, national and international levels. SACMID seeks to play a role in serving the needs of the local communities whenever possible under the purview of national and international rights-based approaches.

- **Innovation and protection of proprietary information;** SACMID supports and encourages innovation by Person or Legal Entity concerned to SACMID in all areas of its activities. SACMID's intellectual property is one of its most valuable assets and the copyrights, and other proprietary information of SACMID must be protected in accordance with the local laws and internationally recognized good practices adapted by the SCAMID. At the same time, each Person or Legal Entity concerned to SACMID must respect the intellectual property rights of others. For the purpose of this Policy, Intellectual Property shall mean Copyrights, Patents, Trademarks, and Trade Secrets of SACMID and other relevant stakeholders of SACMID.

- **Accuracy of accounting records;** SACMID's accounting records must be accurate, detailed and reliable in all material respects. Unrecorded financial transactions are prohibited for SACMID. The records or accounts of financial transactions of SACMID shall not contain any confusing, false, misleading, forged or artificial entries.

- **Anti-fraud and forgery;** SACMID does not tolerate fraudulent behavior or activities, such as embezzlement, fraud, corruption or theft. Such violations will lead to immediate termination of employment and are subject to criminal sanctions as per the laws of Bangladesh. Any forgery shall not be allowed in relation to any document, record, electronic or virtual database, log, receipt, or memorandum either produced or received by SACMID.

1B: SACMID Behavior

SACMID aims to create a working environment where people treat each other with trust and respect and where everyone feels responsible for the results and reputation of SACMID. All Person or Legal Entity concerned to SACMID are expected to refrain from any acts of misconduct. At SACMID we expect the following conduct of Person or Legal Entity concerned to SACMID:

- We treat everybody equally in equal circumstances and do not discriminate based on race, gender, sexual orientation, disability, political convictions, religion, culture, creed or for any other reason, in any way
- we will not engage in harassment, deprivation, exploitation and sexual abuse or threat of abuse; we stay away from and strongly reject any abuse of power;
- we reject any form of violence including but not limited to: bullying, verbal, physical, psychological or sexual harassment, rape, torture, exploitation, intimidation and victimization;
- we show behavior that respects the dignity of others including their (personal) confidentiality;
- we reject behavior that leads to, or could potentially lead to health or security problems for the person themselves or for other people;
- we reject any exchange of money, employment, goods (including but not limited to drugs and alcohol) or services for sex, including sexual favors and/or other forms of humiliating, degrading, compromising or exploitative behavior;
- we respect the dignity of the individual and freedom of association;
- we provide good communication with any Person or Legal Entity concerned to SACMID by means of information and consultation procedures;
- we offer Person or Legal Entity concerned to SACMID the opportunity to report any kind of misconduct.
- Any Person or Legal Entity concerned to SACMID should not work under the influence of alcohol or drugs. Working under the influence of drugs or alcohol possessan unacceptable safety risk to the concerned person's and others' physical and mentalhealth. Drugs may include illegal drugs, controlled substances or misused prescription medication. Person or Legal Entity concerned to SACMID are expected to perform their job or responsibilities or duties free from the influence of any substance that could impair their job performance.
- We therefore prohibit: Working under the influence of alcohol, illegal drugs or controlled substances. Possessing, selling, using, transferring or distributing illegal drugs or controlled substances while working or on the SACMID premises.

1C: SACMID use of equipment, internet, social media and digital platforms

It is SACMID's responsibility to ensure the health, safety and wellbeing of Person or Legal Entity concerned to SACMID based on systematic feedback mechanisms to monitor and to take appropriate measures when deemed necessary.

SACMID's digital safeguarding commitment is to:

- Support Person or Legal Entity concerned to SACMID, to navigate digital spaces and use equipment and digital tools safely and effectively in accordance with good practices by the SACMID's partner organizations (e.g. Free Press Unlimited work).

- Be proactive in promoting digital safety by giving guidance, tools and training to Person or Legal Entity concerned to SACMID where possible and appropriate.
- Take action on digital safeguarding and data protection incidents when the Person or Legal Entity concerned to SACMID is aware of these.

1C.1 DIGITAL SAFEGUARDING

Digital safeguarding refers to the safeguarding policies, procedures and practices relating to online spaces, which might affect offline activities as well. The same safeguarding principles apply to SACMID's programs, initiatives and activities, whether these take place digitally or physically. However, there are specific considerations to take into account with online initiatives, as digital technology has brought about new safeguarding issues.

The following risks should be taken into account when considering digital safeguarding.

Content risks

Risks that are produced as a result of the harmful materials or contents or information or audio-visualization ("Content") that people can access online. People may be exposed to this content actively or passively, and it may produce a harmful effect. Content may be illegal to possess or share according to national law, e.g. sexually exploitative images of children or radicalizing videos. Inappropriate and offensive content is more subjective, and includes but not limited to: commercial adverts or spam; violent, extremist or hateful material; sexually exploitative or sexual material; and content which is discriminatory based on someone's race, ethnicity, creed, nationality, class, socioeconomic status, age, sex and gender identity/expression, sexual orientation, (dis)ability, religion, language, political ideology or other status.

Contact risks

Risks that are produced as a result of encountering others' online behavior. Individuals may have information or data about them shared or may be engaged in ways that lead to harmful consequences. The types of behavior which people may experience include, but not limited to:

- Bullying online or through any electronic medium (e.g. mobile phones);
- Harassment and stalking;
- Ideological grooming;
  - Promoting or expressing hate speech online;
- Exposure to political risks, e.g. government surveillance or having details of online activism shared with authorities in politically oppressed contexts;
- Increased exposure to cybersecurity risks, e.g. by having malicious content shared such as spreading malware, DDoS attack, or attack by apps or other active content or malicious code, or targeted attack such as ransomware attack, phishing attack etc.;
- Harvesting, tracking and illegal sharing and possession of information and data – including having personal data collected, processed or shared without the individual's consent or on another unlawful basis;
- Unauthorized Distribution of private and sexual images, e.g. the distribution of sexually exploitative images or videos without an individual's permission;
- Non-contact sexual abuse and exploitation – including grooming, flashing, being persuaded to perform sexual acts online, and being exposed to sexually exploitative images or videos.
- Obtaining personal sensitive information or data by fraudulent or forgery or impersonation or without informed consent.

Conduct risks
Risks that are produced as a result of people's own online behaviour, which may put themselves and others at risk. People may download something illegally or without permission or without informed consent; may bully, harass or exploit others, unintentionally reveal their location, create and upload sexual material or sexting (send someone sexually explicit photographs or messages via mobile phone). This may also include online activism in politically oppressed or conservative contexts, or breaking confidentiality of closed spaces by reposting, sharing, downloading or in other ways transmitting information that leads to harassment, exploitation, or other types of harms, e.g. reputation harm or physical harm, in another setting (both online and offline).

Technology-based gender-based violence
SACMID recognizes that online harassment, bullying and sexual exploitation can affect anyone, but is most likely to affect women, girls and LGBTQI+ individuals. These groups face an increased risk of violence through digital technology, which can be considered a form of Gender-Based Violence. Person or Legal Entity concerned to SACMID should be aware of common perpetrators and acts of such violence.

Perpetrators include:
- Individuals or groups who target people on an ideological basis such as fundamentalist, extremists, , ultra-nationalists, patriarchal, sexist or homophobic groups.
- Acquaintances, intimate partners or family members who wish to harm someone or exercise power over them.

Acts of violence include:
- Online harassment and trolling.
- Cyberstalking (tracking and monitoring of someone's movements and activities online).
- Hate speech online
- Invasion of privacy by gaining access to phones, devices, and email or other accounts without consent.
- Distribution without consent of private and sexual images, or using these images as leverage and enforcement of power dynamics.
- Online Gender Discrimination
- Online apartheid

1C.2 Roles and Responsibilities on Digital Safeguarding

All Person or Legal Entity concerned to SACMID are required to report any digital safeguarding suspicions or incidences . Failure to report these to a relevant person shall be presumed as a breach of SACMID's policy, and could lead to disciplinary action being taken against employees and the termination of SACMID's relationship with non-employees. There is no obligation for an individual to report any incident that has happened to them.

- **Trustees and Directors:** Hold overall accountability (individual and collective) for this policy and its implementation.

- **Safeguarding Focal/Basic Points:** Provide support to prevent and respond to digital safeguarding incidences alongside their substantive roles. They raise awareness and promote best practices by

supporting survivors and receiving and reporting concerns in a confidential manner within their Affiliate channel.

- **Social media, website, channel, shop, project, programme and campaign managers:** Responsiblefor signing off the creation of official SACMID online accounts and platforms, and for coordinating sign-off of sensitive content as necessary.

-**Project Teams:** Consult with Person or Legal Entity concerned to SACMID in a safe, accessible, and culturally appropriate way to ensure that they are familiar with the SACMID CODE OF CONDUCT, how to raise complaints and concerns, and SACMID's processes and procedures for dealing with these. Project Teams should also clearly explain what goods and/or services those involved in SACMID's work (e.g. project participants) are entitled to, and how they are selected.

1C.3 USE OF EQUIPMENT, INTERNET AND SOCIAL MEDIA

All Persons or Legal Entity concerned to SACMID must adhere to the terms of their employment,engagement and the guidelines when using equipment, internet, social media or digital platforms on behalf of, or belonging to SACMID.

SACMID should carry out a Digital Risk Assessment for all initiatives involving social media or digital platforms, or where SACMID is providing equipment or access to internet. Special consideration should be taken where these initiatives involve children, young people and vulnerable adults, and monitoring of usage may be appropriate.

Where significant risk may exist to individuals (risk of harm, distress, or the infringement of other rights and freedoms), there may be an explicit legal requirement to carry out a Privacy Impact Assessment (PIA). Data Protection Officers or Focal Points appointed by SACMID, can advise on how this may be undertaken.

1C.4 Use of SACMID's internet and ICT equipment

Usage of equipment or access to internet which has been provided by SACMID must take into account the following:

- It is prohibited for anyone to browse, download, access or share content which is illegal, harmful, violent, extremely , hateful, sexually exploitative, abusive, offensive, or otherwise inappropriate using internet or equipment which has been provided by SACMID, unless this is required for their role, e.g. safeguarding and investigator roles.
- Parameters for acceptable usage of equipment should be set by SACMID, and SACMID may use technical means e.g. software, to limit what apps or tools Person or Legal Entity concerned to SACMID are able to access.
- Equipment provided by SACMID should ensure that technical solutions are in place to protect the user from online associated harms, e.g. anti-virus, monitoring and filtering software.
- Appropriate monitoring should take place based on the level of risk of the people involved (e.g. children, young people, vulnerable adults), and the content which they will be coming into contact with.
- SACMID should give advice, support and training on how to mitigate risk when using ICT equipment and internet which it has provided.
- Where SACMID is giving the equipment to Person or Legal Entity concerned to SACMID, e.g. at the end of a project, equipment should be cleaned of any personal data. It should be made clear to them that they are now responsible for the use and maintenance of the equipment.

1C.5 Use of social media and digital platforms

All Person or Legal Entity concerned to SACMID are personally responsible for what they communicate on social media and digital platforms while expressing themselves as SACMID staff or working under the professional capacity of SACMID, and also using SACMID's internet and equipment – both on behalf of SACMID.

Published content is often available for anyone to read, and may reflect negatively on the organization, while those using online platforms as part of SACMID's work may be exposed to harmful content.

- All Person or Legal Entity concerned to SACMID should not behave in a threatening, bullying or abusive way online – whether in a professional or personal capacity.
- Social media, website, channel, shop, project, programme and campaign managers of SACMID are responsible for signing off the creation of official social media accounts or digital platforms related to SACMID's programmes, campaigns or initiatives.
- Person or Legal Entity concerned to SACMID responsible for the creation of online content on SACMID accounts and platforms (e.g. Tweets and Facebook posts) should seek advice and sign-off from these managers or line managers on sensitive content or while they are concerned about the appropriateness of the content.
- When posting potentially upsetting material on SACMID's social media accounts and platforms, content warnings should be given.
- Children and vulnerable adults should not be tagged in online or social media posts without prior consent of their legal guardians.
- If illegal, harmful, violent, extremist, sexually exploitative, abusive, offensive or otherwise inappropriate content is posted in SACMID's groups or platforms, this should be hidden or deleted by group managers/moderators, and where appropriate reported to third-party platform hosts.
- SACMID should develop appropriate relationships with online platform and social media providers where possible, so that content which may put others at risk can be removed swiftly.
- SACMID initiatives using social media should be aware of age limits for corresponding social mediaplatforms (e.g. a campaign using Facebook as a key promotion tool should be aware that the minimum user-age is 13).
- If a profile, group, page or platform is set up directly related to SACMID's programmes, campaigns or initiatives, a minimum of two members of SACMID staff or representatives should oversee the content and activity as moderators. Moderators should remove or edit inappropriate content assoon as possible after it has been posted, and should set up mechanisms to pre-approve content where this is enabled by the third-party provider. Moderators should also provide guidelines on rules of engagement.
- Where possible, Person or Legal Entity concerned to SACMID should not make use of their personal social media accounts to carry out their work for SACMID-related projects, events or initiatives without prior permission of SACMID. Where this does not contravene third- party terms of use, a new account should be opened that enables the staff member to maintain boundaries between their personal and professional lives.
- Person or Legal Entity concerned to SACMID can only use their SACMID email address to set up social media accounts if these will be used on behalf of the organisation. Where this account represents a SACMID initiative, managers should have access to this account, and login details should be shared with other SACMID staff members so that this account can be used as a shared resource.

- For the purpose of official communication from SACMID, Person or Legal Entity concerned to SACMID should not have private conversations with persons under eighteen years of age through email, or through accounts on social media or online platforms . Where children get in touch with SACMID through its official social media or online platform accounts, e.g. to ask for more information about a project, processes should be in place so that at least two other adult staff/employee of SACMID are able to view these messages, and are informed when a message is sent to or received from a child. In other instances, if sending a direct message to a child is unavoidable, e.g. to inform them of a sudden change of itinerary for a SACMID-related event, an adult with a duty of care towards the child (e.g. parent, guardian or teacher) and a relevant SACMID staff/employee (e.g. manager or safeguarding focal point) should be copied into the message.
- SACMID should provide guidelines on settings and privacy to people engaging in digital spaces forSACMID initiatives to protect them from harmful behaviour.
- Sharing online content/work of Person or Legal Entity concerned to SACMID on social media should follow the guidelines on privacy, data protection, informed consent, safe programming and risk management as it has been outlined in this Policy.

1C.6 PRIVACY, DATA PROTECTION AND INFORMED CONSENT

SACMID has a duty of care to protect the digital data and content of Person or Legal Entity concerned to SACMID, even when they make the informed decision to share this content. This duty of care is rooted in privacy law, and includes an obligation to be transparent in explaining how SACMID will use individuals' data, how SACMID considers the risk to individuals, and how SACMID cares for their data throughout the lifespan within which it will be used.

SACMID must take every reasonable precaution to ensure that any digital data or content does not place people at risk or render them vulnerable to any form of harassment, abuse or exploitation.

Research which involves digital elements, such as online surveys or platforms, must be well thought through and appropriate for the context. Special consideration must be given to data protection concerns and mitigating risk to research participants.

1C.6.1 Minimum principles

- SACMID is **transparent, lawful, and fair** with individuals when using their data, and will explain to individuals how it will use data when it collects or obtains it.
- SACMID will only use data for the **purposes for which it was obtained** and then destroy it appropriately. SACMID will not retain or use this information to contact or work with people for any other reason.
- SACMID will only collect the **minimal amount of data** for the purpose at hand.
- SACMID will retain **accurate data** and keep it for **no longer than necessary.**
- SACMID will ensure its data is stored **securely** and access is restricted to as small a number of staff/employee as possible.
- SACMID will always seek written parental **consent prior** to collecting and using data related to children. The consent form must be sensitive to children, it must stipulate what channels the content will be used on, and it must outline that social media content may exist indefinitely unless the parents or child ask for it to be deleted.
- SACMID will only **disclose personal information outside of SACMID** in an identifiable form if explicit consent has been given for this or there is a compelling legal reason (or similar overriding interest) which is considered and risk-assessed.

- SACMID will comply fully with any **local data protection legislation**.
- SACMID will ensure that, from their inception, projects **and activities which involve data** must include a **planned-in consideration** for the protection of confidentiality of data (**security**) and the privacy and agency of individuals (**privacy**).

1C.6.2 Informed consent

SACMID should ensure that informed consent is obtained for the gathering of content which will be shared publicly in the digital sphere. This should ensure that the persons truly understand what they are consenting to, with full knowledge of the possible risks and benefits. The below guidelines for gathering and sharing content online represent a requirement for ethical consent , and which SACMID has committed to.

- For children, SACMID must seek informed consent from a parent or guardian, in addition to attaining informed assent from the child, where they are old enough to understand.
- Adults, children's parents/guardians, and – where possible – children must be given enough context to make this context 'informed'. In particular, they must be able to reasonably understand how their image or likeness may be used, and what the consequences may be.
- Images, stories, recordings or other personal data of children should not be accompanied by identifying information when shared online, e.g. the child's real name or school name. This applies even if a parent/guardian gives informed consent for a child to be interviewed in a way that reveals their identity. Exceptions can only be made in specific circumstances, e.g. where a child has won a prize or led a campaign and this has been widely reported in the media, where a full Risk Assessment has been carried out and the identified risks are minimal, and where informed consent is obtained following this Risk Assessment.
  - Identifying information should not be included when content is shared online where this may put people at risk, e.g. political harassment, targeting by religious extremists.
- A story-gatherer (e.g. interviewer, photographer, video-maker) should exercise judgement and creative skills to tell a powerful story in a way that doesn't reveal the identity of a child, young person, vulnerable adult, or someone who may be put at risk due to e.g. political or religious contexts.
- Participants retain the right to remove any pictures or stories about them from online spaces at any stage and should be made aware of this.
- There must be a practical means for adults, children's parents/guardians, and – where possible – children to contact SACMID to allow them to assert this right.
- Content should receive the appropriate levels of sign-off when gathering content and before sharing it online.
- There are some key areas where SACMID needs to be extremely alert and sensitive to sharing content online as there may be additional risk, and this may be ongoing.
  - Emergency situations – vulnerable, traumatized or orphaned individuals
  - Conflict situations – vulnerable, traumatized or orphaned individuals and,combatants and parties at conflict
  - Abuse – perpetrators or survivors of any form of abuse
  - Crime – perpetrators or survivors of a crime

1C.7 SAFE PROGRAMMING AND RISK MANAGEMENT

i. Digital Risk Assessment

Effective contextual analysis is essential to identify potential risks for employee, agent, director, trustee board member, advisor, client, respondent, beneficiary, affiliate, partner, project participants or service receiver/recipients or others involved in SACMID's work when operating online. Assessed risks, potential consequences and mitigation strategies should be considered before any programmes, campaign, activities or initiatives which have a digital element begin.

Relevant SACMID employee, agent, director, trustee board member, advisor, client, respondent, beneficiary, affiliate, partner, project participants or service receiver/recipients can offer support to ensure that these assessments are gender-sensitive and participatory.

The following elements should be taken into consideration:

- The social, cultural and political context which may increase risk.
- Campaigning, advocacy and influencing work which entails risk of harassment or targeting by political, religious or cultural actors.
- The individual situation of the people involved in SACMID's work – including intersectional factors relating to race, ethnicity, religion, age, sex and gender identity/expression, sexual orientation, (dis)ability, political affiliation, and any other status which may put them at risk.
- When working with children, discussions must address how parents or legal guardians will be informed of any significant risks and involved in decision making before they start their engagement with SACMID.

ii. Risk Mitigation

The extent of the risks identified in the Risk Assessment will determine whether SACMID should mitigate against these by restricting SACMID's online activities, or advising those involved in SACMID's work against online activity. In addition, they should not undertake online activities through SACMID if:

- There is a risk of identification through online activities, where this may put them at risk (e.g. political harassment, sexual abuse, targeting by religious extremists).
- It is deemed to put them at risk of violence (e.g. gender-based violence, political violence).
- It involves risk of accidents which they are unlikely to recognise (e.g. due to lack of awareness of online risks or lack of online experience).
- There is any other restriction specific to local legislation or cultural issues, e.g. internet censoring.
- They are of compulsory school age and this would harm school attendance or academic performance.
- There is a risk of child exposure to illegal, harmful, violent, extremist, sexually exploitative, abusive, offensive or otherwise inappropriate content.
- There is no way for SACMID to mitigate risks.
- The outcome of a Risk Assessment and/or Privacy Impact Assessment indicates that there would be high risk to individuals for these or other factors.

1C.8 CHILDREN AND YOUNG PEOPLE

SACMID recognizes that children and young people are a group who experience specific risks in thedigital sphere, and that special measures should be taken to ensure that they are protected from abuse, harm and exploitation when engaging with SACMID's online work.

Special considerations include:

- SACMID should obtain informed consent from the child and/or parent or guardian of the child for the processing of children's data. An explanation of how the data will be used must be provided.
- Guidelines on informed consent and identification of children must be followed when gathering content to share publicly (see Section 1C.6.2 mkm,,m (??) above for more information).
- SACMID should not support children to engage in SACMID's work through social media or digital platforms when they are under the minimum joining age set by the third-party provider. It is SACMID's responsibility to be aware of minimum age requirements, which vary across third-party platforms (e.g. on Facebook the minimum user-age is 13). For children over the minimum joining age, a Risk Assessment should determine whether social media platforms are the most appropriate way for SACMID to engage with them.
- SACMID should provide guidance and tools to children and young people to protect themselves when using equipment, internet, social media or digital platforms to work and engage with SACMID. Appropriate training should also be provided where possible. This includes, but is not limited to: social media privacy settings, online security, sharing content, and engaging with others online.
- The use of technical equipment, internet, social media or digital platforms not only carries individual and technical risks but also collective and social risks that could increase the gap between people that have access to the digital world and those who do not. It can also push people into groups and promote polarisation, which is particularly relevant for young people who are forming their identities. Whenever SACMID engages with young people in a way that includes digital work, these elements should be considered and discussed with youth participants.

1C.9 SUPPORT FOR SURVIVORS

Survivors are entitled to specialized support services. SACMID commits to referring survivors to competent support services as appropriate and available and according to the wants and the needs of the survivor. Support may include specialist psychosocial support such as counselling, medical assistance, legal counselling. Assistance will be made available regardless of whether a formal internal response is carried out (such as an internal investigation).

PART 2: THE ANTI -FRAUD & CORRUPTION POLICY

Personnel at SACMID offices are personally and collectively responsible for upholding and promoting the highest ethical and professional standards in their work. Everyone has a commitment to prevent fraud, forgery, corruption and unethical business practices. This also applies to board members when representing SACMID and temporary personnel such as consultants and volunteers during their mission with SACMID.

The management on all levels has a responsibility to ensure that all personnel are aware of this Anti- Corruption Policy that they understand what it means in concrete behavioral terms and how it applies to their programme context, e.g. official responsibilities or tasks given.

SACMID implements its tasks in professional manner, without any intention of influencing people's religious affiliation, and do not encourage fundamentalism or support proselytizing activities. SACMID supports people irrespective of culture, gender, sexual orientation, age, functional abilities, ethnicity and political persuasion and have followed SACMID's other policies and related national and international rights-based approaches for the preparation.

For the purpose of this policy, SACMID personnel include all its employees, advisors, agents, dealers, executors and all other relevant stakeholders relevant to the operation and commencement of the activities of SACMID.

2A. Definitions:

- **Corruption:** Corruption is the "offering, giving, soliciting or acceptance of an inducement or reward which may improperly influence the action of any person". In addition, the definition shall also include the definition of corruption underlined by the Anti-Corruption Commission Act, 2004.

- **Fraud:** Fraud is an intentional distortion, deceit, trickery, and perversion of truth or breach of confidence, relating to an organization's financial, material, or human resources, assets, services and/or transactions, generally for the purpose of personal gain or benefit. Fraud is a criminal deception or the use of false representations to gain an unjust advantage. In addition, the definition shall be interpreted under the purview of Penal Code, 1860.

- **Forgery:** Whoever makes any false document or part of a document, with intent to cause damage or injury, to the public or to any person, or to support any claim or title, or to cause any person to part with property, or to enter into any express or implied contract, or with intend to commit fraud or that fraud may be committed, commits forgery. In addition, the definition shall be interpreted under the purview of Penal Code, 1860.

2B. Scope

The Anti-Corruption Policy outlines the key responsibilities of all SACMID personnel in relation to pay respect for the authentication and dedication to the organization with whom they work in the development and humanitarian context. It is designed to assist personnel to better understand the obligations placed upon their conduct, as to prevent any corruption and unethical business practices.

Therefore, all SACMID personnel shall at all times:

- promote the implementation of this Anti-Corruption Policy by contributing towards the creation and maintenance of an environment that prevents corruption and unethical business practices at every step of implementing activities in the organization.

- report immediately any information, concerns or substantial suspicions of breaches of this Policy or any other policies of SACMID, to her/his manager and/or senior management of the offices (or following procedures established by the SACMID's complaints mechanisms), who is expected to undertake prompt investigative measures.

- be aware that failure to disclose or knowingly withhold information about any reports, concerns or substantial suspicions of breaches of this Policy constitutes grounds for disciplinary measures.

- uphold the highest standards of accountability, efficiency, competence, integrity and transparency in the provision of goods and services in the execution of their job.

- cooperate when requested with any investigation into alleged breaches related to this Policy.

2C. Fraud, forgery and corruption

SACMID has a zero-tolerance approach to fraud, forgery and corruption. SACMID personnel shall-

- Conduct all business in accordance with nationally & internationally accepted practices, procedures, laws and uphold the highest standards of accountability and compliance in relations to finances, management and governance, where relevant.

- promote a culture of honesty, neutrality and openness among SACMID personnel and management.

- be transparent in all work-related financial transactions.

- create a work environment where communities and personnel can safely and confidentially raise and report all serious concerns about any suspected fraud and corruption.

Moreover, SACMID personnel shall never-

- take advantage of their position when working with communities, partners or other stakeholders.

- contribute to corruption by giving bribes or receiving them, either in form of money or other benefits, which are intended to give advantages in relation to others.

- steal, misuse or misappropriate funds or property, ensuring that financial and other resources are used solely for the intended purposes. This applies also to any other income generated or fund-raising activities [such as any interest received/earned on the funds].

- engage in illegal transactions, or check forgery, money laundering, taking of commissions and influencing tender in procurement process for improper benefit and theft.

- knowingly support individuals or entities involved in illegal activities.

- allow or encourage any gender disparity in dealing with the matters related to fraud and corruption.

- deliberately destroy, falsify, forge, alter or conceal evidence material to an investigation or make false statements to investigators in order to materially influence or impede investigations into corrupt, fraudulent, coercive or collusive allegations.

2D. Unethical business practices

SACMID personnel shall:

- Always follow transparent, accountable and honest practices when receiving cash donations both from national & international sources earmarked for humanitarian or development purposes.

- Always pay compulsory State taxes and comply with national business law and international standards.

- Always strive for the highest health, safety and environmental standards in all programme work.
- Ensure, where possible, that goods purchased, produced and delivered under conditions that do not involve the abuse or exploitation of any person and have the least negative impact on the environment.

- Always declare any known or potential conflicts of interest to their employer (e.g. any direct relationship with service providers, suppliers of goods or consultants for SACMID programmes, etc.)

Moreover, the SACMID Personnel shall-

- Never use or accept a bribe in the form of money, goods and or services to secure a contract/consultancy for services when dealing with suppliers/vendors in any development or humanitarian work

- Never take part in activities that generate personal, organizational or collective profit such as buying or selling when such activities may affect or appear to affect SACMID credibility or integrity

- Never share in the profits or budget leftovers as kickbacks, cuts or discounts for personal or organizational benefits

- Never accept any gifts or other favors that may influence the performance of personnel functions or duties. Gifts are defined as, but not limited to: services, travel, entertainment, material goods, among others. In order to respect national and local traditions and conventional hospitality, minor token gifts such as pens, calendars, desk diaries, etc. can be accepted.

- Never use illegal labor, child labor and forced labor in any work place.

- Never use or distribute known unsafe products or supplies in any development or humanitarian setting.

- Never provoke, induce, seduce or influence others to conduct above mentioned unethical business practices.

2E. For the procedure on reporting of fraud & corruption see **PART 4: Report & Complaint Procedure.**

PART 3: THE WHISTLE BLOWING POLICY

SACMID is committed to listening to people using our services. We take on feedback, both positive and negative, as a source of ideas for improving our services and other activities.
We are committed to facilitating our clients' right to make a complaint about our service, to appeal a decision we have made that directly concerns them, and to ensuring that their complaint or appeal is fairly assessed and responded to promptly.

Thus, the transparency and accountability are the core issues of any operations conducted or any services offered by SACMID. This policy on collecting feedback from the clients, and complaints and appeals procedures to provide redressed mechanisms for the victims serves the purpose of transparency and accountability for the organization.

3A What is Whistleblowing?

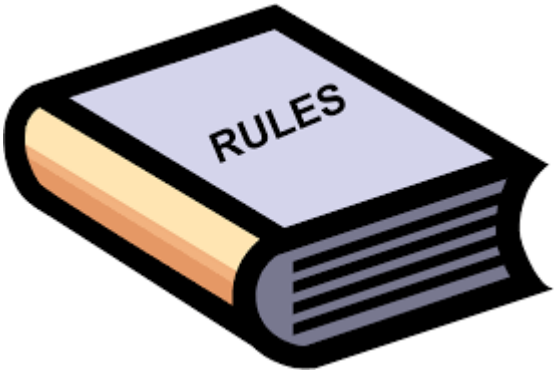
Whistleblowing is confidential disclosure by an individual, or a group of people, of any concern encountered in the workplace relating to a perceived malpractices. The whistleblower must identify himself or herself, as explained later in this document. This will be kept confidential by the concerned authority (Ethics Committee and/or unit) handling whistleblowing.

Examples of malpractices include, but are not limited to:

- a criminal offence, for example fraud causing someone's health and safety is in danger.
- risk or actual damage to the environment
- a miscarriage of justice
- the company is breaking the law, for example does not have the right insurance
- you believe someone is covering up wrongdoing

For the purpose of the abovementioned general and gross malpractices, the malpractice in question shall be in contradiction with this Policy.

If the malpractices is somewhat related to the public interest, then the Public-interest Information Disclosure (Provide Protection) Act, 2011 will be applicable to the extent it does not contradict with this Policy.



3B. Who is a whistleblower?

You're a whistleblower if you're a worker and you report above mentioned malpractices. This will usually be something you've seen at work - though not always. The malpractices you disclose must be in the public interest. This means it must affect others, for example the general public. As a whistleblower you're protected by law - you should not be treated unfairly or lose your job because you 'blow the whistle'.You can raise your concern at any time about an incident that happened in the past, is happening now, or you believe will happen in the near future.

3C. Complaints that do not count as whistleblowing

Personal grievances (for example bullying, harassment, discrimination) are not covered by whistleblowing law, unless your particular case is in the public interest.

Report these under the SACMID Code of Conduct and/or The Anti Fraud & Corruption Policy

3D. Who Does this Policy Apply to?

This policy applies to everyone who carries out work for SACMID, including:

- All members of the Board of Trustees of SACMID
- All employees of SACMID
- All employees working on all programs of SACMID
- All employees of SACMID's partners (including partner NGOs, grantees, sub-grantees, business partners, vendors, suppliers etc.)
- All volunteers of SACMID
- All agents of SACMID
- All Consultants of SACMID
- All Advisors of SACMID

3EWhat is a Protected Disclosure?

A protected disclosure is any communication that discloses or demonstrates an intention to disclose information in good faith that may have evidences of (a) malpractices within SACMID, or (b) any condition that may significantly threaten the health or safety of employees or the public. A protected disclosure may lead to a whistleblowing disclosure.

3F Ethics Committee and its Role

The Ethics Committee will comprise: a) one member form the Board of Trust ; b) Director Operations and; c) Head of the Accounts/Internal Audit. In the absence of Director Operations, the second slot will be filled up by another Board Member. The HR Manager will be secretary of all meetings, and will be kept in the loop by the Ethics Committee throughout the proceedings of the case.


POLICIES

The HR department will be responsible for maintaining the record and documentation of all such proceedings. If any one of the members of the Ethics Committee is the subject of whistleblower's allegations, then he or she will be replaced on the Committee for that case by the Committee.

After conducting investigations, if the Ethics Committee feels or finds that the issue raised by the whistleblower is critical to the operations of SACMID and threatens to have pervasive negative implications, the Committee will escalate the matter to the Board of Trustees for further deliberation.

3G Communication Strategy

Understanding, agreeing upon and complying with the communication strategy is critical throughout the process. An expedient and reassuring communication from an appropriate member of the Ethics Committee to the whistleblower should confirm that the report was received and that it will be handled in accordance with SACMID's policies and procedures.

Generally, it is helpful to appoint a single person or a few individuals as possible to be the primary point of contact with the whistleblower. Initially, for the safety of the investigation team and to preserve evidence and the investigation environment, the alleged perpetrator should not be made aware of allegations. However, after collecting all the necessary evidence, the alleged perpetrator should be notified with a show cause notice to defend himself or herself.

Regarding communications beyond SACMID staff, the Chairman of Audit Committee(e.g.the Treasurer) of the Board of SACMID must receive a notification of the reported event.

All investigations should culminate in an internal report and an assessment of whether communication to donors, partner NGOs, grantees, sub-grantees, business partners, vendors, suppliers, law enforcement officials or other government officials is required or advised.

3H Possible Outcomes

There will be no adverse consequences for anyone who ***does whistleblowing in good faith***.

The following actions may be taken after investigation (mentioned in 4A. Complaint Mechanism) of the concern;

- Disciplinary action (up to and including dismissal) against the wrongdoer dependent on the results of the investigation.
- Disciplinary action (up to and including dismissal) against the whistleblower if the claim is found to be malicious or otherwise in bad faith.
- No action if the allegation proves unfounded, and the committee concludes that the whistleblower did not operate with a malicious intent or in bad faith.

The whistleblower will be kept informed of progress and the outcome of the investigation, within the constraints of maintaining confidentiality or observing legal restrictions generally.

3I Safeguards Guaranteed to a Whistleblower

The Whistleblower is protected from victimization, harassment or disciplinary action as a result of any disclosure, where the disclosure is made in good faith and is not made maliciously or for personal gain.

Disclosures will be investigated fully including interviews with all the witnesses and other parties involved.

The identity of the whistleblower will be held confidential at all stages by the Ethics Committee.

While SACMID can provide internal anonymity, it cannot guarantee this will be retained if external legal action flows from the disclosure.

3J Applicability of the Existing Laws

This policy shall be applied and interpreted unless it is contrary to the **Public-interest Information Disclosure Act (Provide Protection), 2011**.

PART 4: REPORT & COMPLAINT PROCEDURE

4A Reporting Regarding Code of Conduct

Implementation; SACMID takes an active approach to the application of this code and promotes its implementation through the effective communication of its contents to its employees. SACMID monitors the application of this code internally. SACMID promotes the application of this code by monitoring the actions of its partners and stakeholders. In the case that questions arise regarding the interpretation of, or compliance with, this Code, especially for any legal affairs, SACMID Board of Trust (BoT) shall be contacted. The application of the code will be reviewed bi-annually by the Board of Trust, which may decide on necessary revisions or interpretations.

Reporting violations; Any SACMID employee becoming aware of a potential violation of this Code must contact his or her superior or members of SACMID Board of Trust. SACMID will investigate all reported matters with discretion due diligence under this Code. SACMID shall not take any adverse actions, as a result of such reporting, against any employee reporting in good faith what he or she believes to be a violation of this code.

Non-Disclosure Clause: SACMID respects rights to privacy and data protection in all levels of its operation. Any employee of SACMID shall not disclose any internal/secret/confidential organizational data or information without prior permission of SACMID authority

Sanctions; Violation of this code may lead to issuance of a warning, temporary suspension from services and benefits, termination of employment and payment(penalty) of damages. In case of violation of any sections of this Code, SACMID employee gives his or her consent to form an Arbitral Tribunal as per the Arbitration Act 2001 of Bangladesh. Any decision given by the Arbitral Tribunal shall be binding on all the parties concerned. Additionally, certain violations of a criminal nature can lead to criminal sanctions, such as fines or imprisonment by the relevant authority under the applicable criminal laws of Bangladesh.

Compliance and Coherence; This Code shall be implemented and interpreted in compliance and coherence of all other guidelines or principles of SACMID.

4B Reporting Regarding Fraud and Corruption

The duty to report is the responsibility of all staff to report suspected, actual or attempted fraud or corruption. Any staff who discovers or suspects dishonest or fraudulent activity has a duty to report this immediately. He/she should not attempt to investigate suspected fraudulent activity him-/herself. The reporting staff may decide to remain anonymous. No information concerning the suspected fraud or status of an investigation should be shared with other persons. Under no circumstances should any reference be made to 'the allegation', 'the crime', 'the fraud', 'the forgery', 'the misappropriation' or any other specific reference. The reporting individual will: not contact the suspected individual or organization in an effort to determine facts of demand restitution; not discuss the case, facts, suspicions, or allegations with anyone, unless specifically asked to do so. All involved treat all information received confidentially.

1. We encourage feedback or complaint in order to improve our operation, conduct, service, commencements, implementation and procedures. Feedback or complaint can be provided to us by; staffs, members, associates, clients, agents, service receivers, partners or stakeholders and partners on their initiative or in response to requests by our organization towards the staffs, members, associates, clients, agents, service receivers and partners.

2. We make it as easy as possible for people to provide feedback or complaint, and ensure anonymity to people who do, unless they agree otherwise. Our feedback or complaint processes include:

- Feedback or complaint either can be written or sent through email, to be sent either to formal mailing address or email address of the Executive Director/Overall incharge of SACMID.
- Written feedback or complaint must be signed and dated by the complainant himself/herself.
- Feedback or complaint sent through email must be sent from email ID of the complainant himself/herself.
- The feedback or complaint shall be constructive, informative, suggestive and free from any threat/undue influence/intimidation/defamatory/incitement to any hatred or crime/unauthorized disclosure of personal data or confidential information.
- The feedback or complaint must disclose the sender's identity and contact details.
- Both the sender and SACMID shall ensure confidentiality of the Feedback or Complaint.
- However, SACMID may disclose or share the contents of feedback or Complaint with its staffs, members, associates, clients, agents, service receivers and partners, subject to Pseudonymzing the identity of the Feedback sender.

3. We want our staffs, members, associates, clients, agents, service receivers, partners or stakeholders to feel able to voice their dissatisfaction with any aspect of our operation, conduct, service, commencements, implementation and procedures, and to be confident that we will manage their feedbacks or complaints well and respond quickly and appropriately. All staffs, members, associates, clients, agents, service receivers, partners or stakeholders are informed of their rights and responsibilities and our complaints and appeals processes at the earliest possible stage of their involvement with our operation, conduct, service, commencements, implementation and procedures.

4. We keep records of feedback or complaint in our Feedback Register Book and Complaint Register Book respectively. After receiving the feedback or complaint, SACMID will process and get back to the concerned feedback or complaint sender (or person) within sixty

days of receiving such feedback either in written or replying to the email sent by the Feedback or Complaint sender.

5. The SACMID shall form a Feedback Management and Complaint Redressal Team for proper, speedy and smooth disposal of feedback or complaints. While dealing with the feedback or complaint, the Team shall follow:

Purpose Specification: The Team shall only focus on the purpose of dealing with Feedback and Complaint, not otherwise;
Purpose Limitation: The Team shall collect data or information only up to the extent necessary to deal with Feedback and Complaint
Bar on automated processing of data: While processing the data or information on Feedback or Complaint received, the Team shall not use of automated means of processing such data or information.
Right to be forgotten: After processing the data or information related to Feedback or Complaint received, SACMID may keep that data or information up to two years, after then the data and information shall be deleted from the record of SACMID.

6. SACMID will never discontinue, reduce, or in any other way take any recriminatory action in relation to a staffs, members, associates, clients, agents, service receivers, partners or stakeholders making a feedback or complaint. SACMID will only take action, if a feedback or complaint raises an issue, to ensure the safety of staffs, members, associates, clients, agents, service receivers, partners or stakeholders, or to prevent harm to the same.

7. The Decisions of the Team is subject to approval of the Executive Director/Executive head of SACMID.

8. In case of any feedback or complaint against the Executive Director of SACMID, the Trustees and Donor Partners of SACMID shall form such Feedback Management and Complaint Redressal Team and their decision shall be final subject to Appeal under Section 4 of this Policy. The provisions of Section 3.7 of this Policy shall not be applicable here.

4C Reporting Regarding Whistleblowing

Any personnel of SACMID and its beneficiaries as well as the other stakeholders can make complaint against any corruption, fraud activity or any unethical business practice conducted by any personnel, board members, temporary personnel such as consultants and volunteers during their mission/employment/engagement with SACMID.

4D Anonymous and Malicious Complaint

If a person lodging a complaint chooses to remain anonymous, SACMID will only be able to receive the complaint, but will not be able to respond or guarantee an investigation.

4E Confidentiality clause:

Complaints shall always be treated with confidentiality. Name and contact details shall not be revealed to any person outside the investigation.

However, the identity and contact details of the complainant may be disclosed as per the directions of complaint management authority or by order of any formal judicial authority. Such revelation shall only be done in order to maintain fairness of such trial.

If a person lodging complaint that is malicious, any investigation underway must be stopped immediately and disciplinary actions are taken if SACMID staff's makes the malicious complaint.

4F Complaint handling and response

Any complaint against any fraud, forgery, corruption or unethical business practice will be handled in line with the complaint and response mechanism developed and prescribed by SACMID from time to time.

4F.1 Raising the Concern

The Ethics Committee can be contacted through email and postal mail by any individual or group of people to raise a concern, show intention to disclose or make an actual discloser. The Ethics Committee is then bound to consider the submission.

4F.2 Investigations

Once the whistleblower makes it clear that s/he is making the disclosure within the terms of SACMID's Whistleblower Policy, the Ethics Committee will consider the matter and take the necessary action to investigate the disclosure.

4F.3 Dealing with Malicious Whistleblowing

All whistleblowing disclosures made to the Ethics Committee will be treated as confidential, unless the Committee concludes that the allegations were malicious, malafide or not in good faith.

Examples of malicious whistleblowing include, but are not limited to, allegations that are based on:

- Misogyny (e.g. not wanting to report to, or work with, a member of the opposite sex)
- Religious or cultural or ethnic beliefs
- Hearsay
- Personal dislike or dispute
- Documents that are either subject to forgery (e.g. email threads, photocopies etc.) or lie outside the legal ambit (e.g. telephone transcripts obtained from phone companies without a warrant)
- Done in violation of any laws of the land, e.g. violation of the Official Secrets Act 1923

In case the whistleblower is deemed by the Ethics Committee to have acted maliciously or malafidely or not in good faith, the whistleblower's identity will be disclosed and no extra care will be taken to hide the corrective measures taken against him/her, which may include, but are not limited to:

- A financial penalty and/or termination if the malicious whistleblower is a SACMID employee.
- Scaling down or termination of the existing grantee, sub-grant or program partner or blacklisting of the party from being eligible for future grants, if the malicious whistleblower is a sub-grantee
- Legal action including defamation charges

4F.4 Preliminary Steps for Investigation and Documentation of Allegations

Disclosing information related to the investigation of a whistleblowing event is a breach of confidentiality and may put the whistleblower at risk. Therefore, inquiries and comments about an allegation will be made within the whistleblower database that will be maintained with Human Resources (HR) at SACMID office under lock and key. Notes will be taken of all discussions about the whistleblower report, but will be documented in a separate whistleblower case file with HR, including specific details sufficient to preserve a record of SACMID's treatment of the allegations and the case chronology.

SACMID requires whistleblowers to identify themselves by providing their name, date of birth, NID number and phone number. Anonymous calls shall **neither** be entertained **nor** investigated, in order to guard against potential abuse of this policy.

The Ethics Committee will determine the preliminary steps as under:

- Identifying who will take the lead on the investigation
- Determining how to best preserve confidentiality
- Identifying who, outside the Ethics Committee, should be included in the correspondence and process.
- Assigning who will be the lead in terms of keeping the Ethics Committee informed on progress

It is important at this time for the Ethics Committee to assess the materiality of the alleged malpractices, and whether it was allegedly perpetrated by exploiting a one-time, temporary gap in internal controls, or a systemic weakness that is present in one department or project, other departments or partner offices. If the allegation is material or indicates a potential systemic weakness, the team must determine if operations should be suspended, modified to reduce the risk of further loss or the weakness addressed and fixed.

***4F.*5 Conducting Investigation**

The matter must be acted upon by the Ethics Committee when any of the following conditions are met:

- The matter is the result of a significant internal control or policy deficiency that is likely to exist in other units within SACMID.
- The matter is likely to receive media or other public attention.
- The matter involves the misuse or abuse of SACMID's resources or creates exposure to a liability in potentially significant amounts.
- The matter involves potential loss of donor funds.

- The matter involves allegations or events that have a significant possibility of being the result of a criminal activity (such as misappropriation of cash).
- The matter involves disregard of SACMID's policies.
- The matter is judged to be significant or sensitive for other reasons.

Having considered the conditions, the Ethics Committee will follow the steps as under:

- Give the whistleblower the opportunity to present his or her case
- Look at the merit of the case as per the conditions for moving on a Whistleblower Disclosure
- If an investigation is warranted, set out a timetable
- Identify witnesses as needed
- Speak with the subject(s) of the disclosure, as needed
- Analyze findings
- Come to conclusions (systematic malpractice or isolated incident)
- Determine action to be taken against whistleblower or subject, if any
- Hand over recorded action to appropriate person or department

If the Ethics Committee concludes that the malpractice or control weakness relates to operations, the findings should be forwarded to the CEO/Director of SACMID.

If the Ethics Committee concludes that the malpractice or the control weakness is systemic in nature or is policy or strategy related, the findings should be taken to the Board of Trustees.

4F.6 **Procedures on Appeal:**

i. Appeal against the decision on complaint filed to SACMID, can be filed to Appellate Team within 30 (thirty) days of getting such decision given by the Team.

ii. Only the aggrieved person, who filed the complaint, can make appeal to Appellate Team.

iii. To process and deal with the Appeal from the Complainant, The Appellate Team shall follow similar procedures mentioned in Sections 3.2, 3.3, 3.4, 3.5 and 3.6 of this Policy.

iv. Decisions of Appellate Team Shall be binding upon all the parties concerned to the Appeal.

v. The Decisions of Appellate Team is subject to approval of the Executive Director of SACMID.

vi. In case of Appeal against the Executive Director of SACMID, the Trustee Boar Members and Donor Partners of SACMID shall form such Feedback Management

and Complaint Redressal Team and their decision shall be final subject to Appeal under Section 4 of this Policy. The provisions of Section 4.5 of this Policy shall not be applicable here.

vii. Apart from availing Feedback Management and Complaint Redressal mechanisms under this Policy, any staffs, members, associates, clients, agents, service receivers, partners or stakeholders and partners can always appeal for before any proper forum established under the Laws of the Land.

viii. This Policy shall be applicable in compliance with other policies, procedures, guidelines of SACMID

ix. This Policy shall not be applicable to the extent it contradicts with existing laws of Bangladesh.

BREACHES OF THE POLICY

Breaches of this Policy shall not be tolerated and may result in disciplinary procedures, change of duties, termination of employment or relationship, and possible legal proceedings, for SACMID employee, agent, director, board members, advisor, client, respondent, beneficiary, affiliate, partner, project participants or service receiver or people working in SACMID's name.

SACMID will take action against anyone or entity, whether they are the subject of a complaint or not, who seeks to or carries out retaliatory action (such as, but not limited to, harassment, intimidation, unfair disciplinary action or victimization) against complainants, survivors or other witnesses. Employees who are found to do this will be subject to disciplinary action, up to and including termination of employment. Others who work with SACMID may have their relationship with SACMID terminated.

If a SACMID employee is found to have made an allegation that they knew to be false they will be subject to disciplinary action, up to and including termination of employment. Others who work on behalf of SACMID will be subject to action that may result in the termination of their relationship with SACMID.

CONCLUSION

In case of any confusion arises to interpreting or implementing or changing or altering or modifying or rectifying this policy, the Board of the Trustees/ Directors of SACMID shall hold all the authority to do such.

This policy shall be applicable in line with the other relevant policy, rules & regulation of SACMID and also shall comply with relevant national tools, laws, policies and regulatory frameworks. Therefore, if any provision, article or rules contradicts with any national rules and regulation, that/those will be automatically deactivated without any prior concern. For the wellbeing of the organizational transparency and accountability authority/management of SACMID can change/replace/ include/exclude any provision or article or rules of this policy with prior concern of its higher management.