Confidential Information and Data Protection Policy

West End Towers, Kanjata Road
Off Muthangari Drive
/ Waiyaki Way

Tel: +254 0703 033 394
Email: info@aecfafrica.org
Web: www.aecfafrica.org

Twitter: @AECFAfrica
Facebook: The AECF

Document Review Schedule

Initial Approval

Document Name:	**AECF Confidential Information and Data Protection Policy**
Document Number:	**AECF.2021.06.005**
Document Version:	**1.0**
Document Owner:	**Legal**
Document Date:	**2 April 2021**
Approved By:	**AECF Board**
Approval Date:	**……**
Effective Date:	**…….**
Applicable To:	**All AECF Staff and Partners**

Amendment and Approval

Document Version			
Revision Date:			
Change Description:			
Reason for Change:			
Change Owner:			
Approved By:			
Approval Date:			
Effective Date:			

Amendment Instructions and Version Control

a) The Initial document is version 1.0

b) Subsequent amendment / addition of paragraphs will change the second part (0) of the Document Version to 1.1 and increase with subsequent changes in paragraphs.

c) Subsequent amendment / addition of clauses will change the first part (1) of the Document Version to 2.0

1. POLICY STATEMENT

1.1. AECF needs to gather and use certain information about individuals, including Staff members, business contacts, consultants, suppliers, investees and other people AECF has a relationship with or may need to contact (hereinafter "Stakeholders").

1.2. The AECF is committed to the protection and safeguarding of Confidential Information and Data obtained from its stakeholders and acknowledges that it has a duty to ensure that its programs and operations are conducted in a manner that upholds high levels of privacy and confidentiality. In that regard, AECF commits to ensure:

1.2.1. Confidentiality of information;

1.2.2. Integrity and availability of information;

1.2.3. Compliance with data protection laws and regulations;

1.2.4. Information security;

1.2.5. Provision of awareness trainings; and

1.2.6. Breaches of information protection, whether actual or suspected, are reported, investigated and any risks attendant thereto mitigated.

1.3. AECF shall comply with the data protection principles, which are:

1.3.1. **Lawfulness, Fairness and Transparency:** Personal Data must be processed lawfully, fairly and in a transparent manner.

1.3.2. **Limitation:** Personal Data must only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

1.3.3. **Minimal Processing:** Personal Data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. Where possible, AECF must apply anonymization to Personal Information to reduce the risks to the Data Subjects concerned.

1.3.4. **Accuracy:** Personal Data must be accurate and, where necessary, kept up to date; reasonable steps must be taken to ensure that Personal Data that is inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay.

1.3.5. **Storage Period Limitation:** Personal Data must be kept for no longer than is necessary for the purposes for which the Personal Data is processed.

1.3.6. **Integrity and Confidentiality:** Appropriate technical or organisational measures (such as staff training, data encryption and backup amongst others) must be adopted to ensure security of Personal Data, including protection against accidental or unlawful destruction, loss, alteration, unauthorised access, or disclosure.

1.3.7. **Security:** Personal Data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

1.3.8. **Accountability:** Data Controllers must be responsible for and be able to demonstrate compliance with the principles outlined herein above.

2. PURPOSE OF THE POLICY

2.1. The Policy describes how Personal Data must be collected, handled, and stored to meet AECF's data protection standards in compliance with the Applicable Regulations.

2.2. The Policy applies to fully or partially automated Processing of Personal and Confidential Information, as well as manual processing in filing systems unless the Data Protection Act provides for a broader scope. The Policy also applies to all AECF Staff Data in hard-copy format in the jurisdiction in which the Information is held.

2.3. We recognize that local legislation applicable to AECF's Stakeholders may vary from country to country. This Policy, however, sets out AECF's minimum standards and may exceed the requirements of local legislation. In addition, the Policy is applicable to all AECF Staff, Stakeholders and Partners wherever they live and work.

3. SCOPE OF THE POLICY

3.1. This Policy applies to all Information processed by AECF, including but not limited to Information of:

3.1.1. AECF Staff, Partners and Directors.

3.1.2. Clients and client employees; and/or

3.1.3. Third Parties dealing with AECF.

3.2. The Policy governs everyone who Processes Information in:

3.2.1. The course of their work with AECF; and/or

3.2.2. Providing services for or on behalf of AECF.

4. OBJECTIVES

4.1. The key objectives of the Policy are as follows:

4.1.1. All Users to understand their responsibilities around the protection of Personal and Confidential Information;

4.1.2. To adequately protect Information Assets against loss, misuse or abuse;

4.1.3. Protection of Information incidences, when they occur, are detected, reported, and ensuring that they are investigated in an efficient and effective manner to ensure that any damage or loss of Information as a result of such incident is minimized and mitigated in the most efficient manner;

4.1.4. Establish a set of principles to assist in the compliance with applicable laws, regulations, statutes, and contractual obligations related to the processing and protection of information;

4.1.5. Provide rules and standards for the protection of AECF Information Assets and use of Information systems, as well as protection from unauthorised access or damage of such AECF Information Asset and/or system;

4.1.6. Supports established processes to access Personal Information; and

4.1.7. Protection of Information threats to business operations to be continually assessed, ensuring threats are identified and managed on a risk assessed basis with appropriate risk controls.

5. ROLES AND RESPONSIBILITIES

5.1. Protection of Information and Personal Data is a team effort and involves the participation and support of all Stakeholders. It is the responsibility of all Stakeholders to know and understand the content of this Policy. The responsibilities of all the Stakeholders include, but are not limited to:

5.1.1. Protection of Information;

5.1.2. Compliance with this Policy and applicable legislation;

5.1.3. Appropriate and responsible use of Information; and

5.1.4. Reporting of Information Protection violations and non-compliance with this Policy.

6. DEFINITIONS

6.1. **Applicable Regulations** means the Data Protection Act.

6.2. **Anonymization** means the removal of personal identifiers from personal data so that the data subject is no longer identifiable.

6.3. **Confidential Information** means irrespective of its format:

6.3.1. any Information: i) which is a trade secret or proprietary in nature used in relation to the technology, business, marketing products, processes, services or operations of AECF, Stakeholders and/or Partners (Herein referred to as Party(ies)); ii) of a trade, commercial, financial and managerial information nature; iii) any Information designated as confidential by the Party(ies);

6.3.2. but excludes any Information that:

6.3.2.1. is or becomes publicly available, except by a breach of this Policy;

6.3.2.2. is disclosed to either Party by a third party and in respect of which the Party receiving the Information (Receiver) reasonably believes, the third party is legally entitled to disclose such Information;

6.3.2.3. was known to or in the possession of either Party without obligation of confidence before it received the Information from the other;

6.3.2.4. was developed by either Party independently of any disclosures previously made by the other Party and in circumstances which do not amount to a breach of the provisions of this Agreement;

6.3.2.5. is disclosed with the other Party's Consent; or

6.3.2.6. is required to be disclosed by law, judicial order, any rules of court, an applicable tribunal or regulatory body, or under any professional obligation or requirement, provided that, in these circumstances, the Receiver shall (i) inform the Party disclosing the Information (Discloser) of the requirement to disclose prior to making disclosure; (ii) disclose only that portion of the Confidential Information which it is legally required to disclose; (iii) use reasonable endeavours to protect the confidentiality of such information to the widest extent lawfully possible in the circumstances; and (iv) co-operate with the Discloser if the Discloser elects to contest such disclosure.

6.4. **Consent** means any manifestation of express, unequivocal, free, specific and informed indication of the data subject's wishes by a statement or by a clear affirmative action, signifying agreement to the processing of personal data relating to the Data Subject.

6.5. **Data** means Information which:

6.5.1. is processed by means of equipment operating automatically in response to instructions given for that purpose;

6.5.2. is recorded with intention that it should be processed by means of such equipment; and

6.5.3. is recorded as part of a relevant filing system.

6.6. **Data Controller:** An organisation or individual that is in control of when, why and how Personal Information is processed and is legally responsible for the use and protection of that data. AECF will frequently be a Data Controller and remain responsible for Personal Data even if AECF is using a third-party Data Processor (e.g., another organisation or individual such as a supplier, partner, or contractor) to carry out the processing.

6.7. **Data Process/Processed/Processing:** as required by the context includes but is not limited to the following actions related to the Information - obtains, records, stores, provides, uses, destructs, and analysis of Data.

6.8. **Data Processor** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Data Controller.

6.9. **Data Protection Act or DPA** means the Data Protection Act, Act No. 24 of 2019 of the Laws of Kenya and any subsidiary legislation thereto.

6.10. **Data Subject(s):** means Data which relates to a living individual (Personal Data) who can be identified, directly or indirectly:

6.10.1. From the Data through an identifier, such as but not limited to: a name, image, an identification number, location data, or an online identifier (e.g. IP address), or

6.10.2. From the Data in combination with other identifying information, which is in the possession of, or is likely to come into the possession of, the Data Controller.

6.10.3. Data Subject may include factual information (e.g. name, address, date of birth) about the Data Subject as well as an opinion or any indication of the intentions of any other person in respect of the Personal Data.

6.11. **Personal Data** that has been pseudonymised – i.e. coded in such a way that it cannot be linked to a Data Subject without the use of additional information – may still be considered Personal Data depending on how difficult it is to attribute to a particular individual.

6.12. **Information Assets:** means all Systems, Electronic Devices, and Information in whichever form (electronic, audible, hard copy or physical) which AECF owns or is responsible for, including AECF Information and Third-Party Information.

6.13. **Information:** means information maintained in Information Assets, including all Information that AECF is responsible for belonging to Data Subjects and includes Personal Information and Special Personal Information.

6.14. **Negligence:** means an action by a staff member which is in contravention with any of the requirements of this Policy in terms of the Safeguarding, Processing or Using of Information and/or Information Assets.

6.15. **Partners:** Includes all donors, grantees, collaborators, suppliers, consultants, sub-contractors, or any parties with a contractual relationship with AECF.

6.16. **Personal Information:** means Information of a living individual or existing entity.

6.17. **Protection of Information:** means the preservation of Confidentiality, Privacy, Integrity and Availability of Information Assets.

6.18. **Sensitive Personal Data** means Information concerning a child and Data revealing Personal Information concerning the race or ethnic origin, health status, biometric data for identification purposes, sex or sexual orientation marital status, family details (including names of the natural person's child(ren), spouse(es), DNA, or criminal behaviour of a Data Subject.

6.19. **Staff** mean individuals who work for AECF either on full time or part time basis for wages and salary.

6.20. **Stakeholder** means individuals, including staff members, business contacts, donors (where applicable), consultants, suppliers, investees and other people AECF has a relationship with or may need to contact.

6.21. **User:** means anyone who has received AECF approval to access or receive any AECF Information Assets. Users include AECF Staff, Partners and Third Parties (that is, individuals who are not employed by AECF, for example contractors, temporary Staff and vendors).

7. SAFEGUARDING OF INFORMATION/DATA PROTECTION

The following principles underpin AECF's safeguarding functions, actions and decisions. All Staff, Partners, Stakeholders and Users are expected to adhere to these principles.

7.1. Lawfulness

Personal Information must be Processed in a lawful manner and in good faith in compliance with the provisions of this Policy and any Applicable Regulations, statutes and contractual obligations. Data Processing may only take place if and insofar as sufficient legal basis exists for the processing activity.

7.1.1 Principles

7.1.1.1 The Data Subject has given his or her Consent;

7.1.1.2 The Processing is necessary for the performance of a contract with the Data Subject;

7.1.1.3 To meet legal compliance obligations;

7.1.1.4 To protect the Data Subject's vital interests; or

7.1.1.5 To pursue AECF's legitimate interests.

7.1.2 Consent to Data Processing

7.1.2.1 Personal data can only be processed following the consent by the Data Subject. Before giving consent, the Data Subject must be informed of his/her rights in accordance with this Policy and the Applicable Regulations. The declaration of consent must be obtained in writing or electronically for the purposes of documentation and record retention. In some circumstances, such as telephone conversations, consent can also be given verbally in which case it must be recorded. The Data Subject has the right to withdraw Consent at any time and AECF must to honour this promptly. Such withdrawal does not affect the lawfulness of the Processing done prior to such withdrawal.

7.1.2.2 Where the collection of Personal Information relates to a child under the age of 18, AECF must ensure that parental consent is given prior to the collection and processing of such Personal Information.

7.1.2.3 Information may be Processed without consent in the following circumstances:

7.1.2.3.1 Processing is necessary for the establishment, exercise, defence or compliance of a right or obligation in law;

7.1.2.3.2 Processing is done for historical, statistical or research purposes; and

7.1.2.3.3 The Data Subject(s) has deliberately made the Information public.

7.1.3 Data Processing pursuant to legal authorization or obligation

7.1.3.1 The processing of Personal Information is also permitted if national legislation requests, requires, or allows this. The type and extent of Data Processing must be necessary for the legally authorized data processing activity and must comply with the Applicable Regulations.

7.1.3.2 Either before or at the time of collection of any Information, AECF, Partners, Stakeholders and Users are required to inform Data Subjects about:

7.1.3.2.1 The kind of Personal Information AECF collects;

7.1.3.2.2 The reason for collecting Personal Information;

7.1.3.2.3 The purpose of the Processing Personal Information;

7.1.3.2.4 the Data Subjects' rights in relation to the Personal Information;

7.1.3.2.5 security measures taken in relation to the Personal Information;

7.1.3.2.6 whether AECF transfers Personal Information to third parties; and

7.1.3.2.7 the retention period and any potential transfers of Personal Information outside Africa.

7.1.4 Information quality and accuracy

7.1.4.1 AECF Staff and Partner(s) shall:

7.1.4.2 Take reasonable measures to determine that the Information Processed is complete, accurate, not misleading and up to date;

7.1.4.3 If the Data Subject(s) requests any Information to be corrected – investigate the request and respond thereto. If AECF and/or Partner(s) are in disagreement with the request, link the request with the Information to ensure that it will be read with an indication that the Information is disputed but not changed. Where changes are made that might impact decisions made on Information Processed prior to the change – parties that may have taken such decisions must be notified of the changes.

7.1.5 Collect the Information directly from the Data Subject

Personal Information must be collected directly from the Data Subject(s) unless the following exceptions apply:

7.1.5.1 The Information is contained in a public record;

7.1.5.2 The Data Subject/s has deliberately made the Information public;

7.1.5.3 The Data Subject/s has consented to the collection of the Information from another source;

7.1.5.4 The privacy interests of the Data Subject/s are not prejudiced; and

7.1.5.5 Collection from another source is necessary to avoid prejudice of the maintenance or enforcement of a law, court proceedings, interests of national security or legitimate interests of a processor that determines the purpose and means of processing the Information.

7.1.6 Keeping the Information Processed relevant

7.1.6.1 AECF Staff and Partners shall Process Information relevant to the specific purpose(s) it is collected for; and

7.1.6.2 Information must be limited to what is minimally required for the purpose.

7.1.7 Processing of Sensitive Personal Data

The processing of Sensitive Personal Data must be expressly permitted or prescribed under Applicable Regulations. Processing of such Data by the AECF may be permitted in particular if the Data Subject has given his/her express Consent, if the processing is necessary for asserting, exercising or defending legal claims with respect to the Data Subject or if processing is necessary for the Data Controller to fulfil its rights and responsibilities in the area of labour and employment law.

7.1.8 Purpose Limitation

Personal Information may be processed only for the legitimate purpose that was defined before collection of the Data. Subsequent changes to the purpose of processing are only permissible subject to the requirement that the processing is compatible with the purposes for which the Personal Data was originally collected.

7.1.9 Data Minimization

Any processing of Personal Data must be limited, both quantitatively and qualitatively, to what is necessary for the achievement of the purposes for which the data is lawfully processed. This must be taken into account during the initial data collection. If the purpose permits, and the effort is in proportion to the objective pursued, anonymized or statistical data must be used.

7.1.10 Accuracy of Data

The Personal Information stored must be objectively correct and up to date. Appropriate measures must be adopted to ensure that incorrect or incomplete data is deleted, corrected, supplemented or updated.

7.2. Safeguards to ensure Information protection

7.2.1 Classification, Labelling and Handling of Information

7.2.1.1 All Information must be classified and labelled by the owner, collector, creator, receiver or the transmitter of such Information in order to determine what level of protection must be applied to the Information.

7.2.1.2 Subject to Appendix 1, Information is classified into:

7.2.1.2.1 Public; and

7.2.1.2.2 Confidential.

7.2.1.3 Information must be handled in accordance with its classification and labelling.

7.2.1.4 Any Information that is not classified or labelled will default to Confidential Information and must be handled accordingly – until classified and labelled otherwise. Information must be labeled in accordance with the Classification categories as identified by the ICT Manager.

7.2.2 Passwords

7.2.2.1 The passwords that give you access to the AECF Systems must be kept secure in order to safeguard Information.

7.2.2.2 This standard explains how AECF expects you to treat your password, and the minimum standards that apply when setting a password.

7.2.2.3 AECF Staff and Users should ensure that the password(s):

7.2.2.3.1 Have a minimum of eight (8) characters;

7.2.2.3.2 Are changed at least every 90 days. In the event of AECF Staff or Users not being able to change a password for any reason, including absence from a duty station, such Staff or User must promptly inform the ICT Manager and request that the validity period of the password be extended. The ICT Manager or their designate has the authority to approve or reject all such requests;

7.2.2.3.3 Are different to the previous five (5) used;

7.2.2.3.4 Are a combination of at least one of each of the following four (4) character types: -

7.2.2.3.4.1 Upper case characters (A-Z)

7.2.2.3.4.2 Lower case characters (a-z)

7.2.2.3.4.3 Numeric characters (0-9) or

7.2.2.3.4.4 Special characters (;!$@%& etc.)

7.2.2.4 Stronger passwords shall be utilised for System and Security Administrator accounts. This means that the password should:-

7.2.2.4.1.1 Have a minimum of eight (8) characters; minimum of twelve (12) characters are recommended;

7.2.2.4.1.2 Be changed at least every 60 days. Service account passwords should be changed at least annually;

7.2.2.4.1.3 Be different to the previous five (5) used;

7.2.2.4.1.4 Be different to all passwords used in the past six (6) months;

7.2.2.4.1.5 Not be identifiable with the User (such as first name, last name, spouse name friends, relations, colleagues, or other easily guessed names);

7.2.2.4.1.6 The length and composition of passwords will be automatically enforced by the system at the time of construction;

7.2.2.5 It is recommended to use long passphrases or sentences rather than passwords. A passphrase uses a string of words rather than a single word, or randomised alpha and numeric characters (e.g. “all good@!*”) For Systems requiring additional security, the use of two factor authentication (2FA) such as the use of one-time passcodes generated by a token or sent via SMS to a user’s phone, or the use of digital certificates or biometrics, is recommended. Such additional security is recommended for situations including:

7.2.2.5.1.1 Authenticating users connecting via remote access solutions;

7.2.2.5.1.2 Authenticating users connecting to perform administrative tasks;

7.2.2.5.1.3 Authenticating users connecting to high-security environments.

7.2.2.6 Users will maintain the secrecy of any passwords that give access to organization's information resources.

7.2.2.7 Passwords should be changed immediately if they become, or are suspected of having become, compromised.

7.2.2.8 Passwords shall not be shared with another user unless required for legal or emergency purposes. In such cases, responsibility for any misuse will remain with the owner of the User ID.

7.2.2.9 Passwords should not be written or stored either physically or electronically in plain text or unencrypted.

7.2.2.10 Passwords should be masked (i.e. should appear as ***** or similar) on the computer screen when users are entering them.

7.2.2.11 Initial passwords for all new Staff or User IDs, or reset passwords assigned when a user forgets their password or when they become, or are suspected to have become, compromised, shall be given to users in a secure manner. Passwords can be reset using the secure "AD Self Service" utility. The use of third party or unprotected (clear text) e-mail messages should be avoided.

7.2.2.12 When provided with a password, a Staff or User shall be required to change it to a different password that they choose, immediately after they next log onto the System.

7.2.2.13 System and Security Administrator passwords (e.g., root, enable, Administrator, System) should be reviewed and updated/revoked prior to any change in administrative responsibility, such as the current administrator leaving the organisation or changing roles.

7.2.2.14 Passwords should not be set to "never expire".

7.2.2.15 Default AECF Staff or User IDs and passwords should be immediately altered following installation of systems or software.

7.2.2.16 The Staff and User IDs for users with privileges such as root, administrator or supervisor should not be suspended as their suspension could create a denial of an essential service. Instead a time delay shall be implemented after each invalid attempt to make brute force guessing attacks more difficult.

7.2.2.17 If there has been no activity on a computer terminal, workstation or desktop computer for at least fifteen (15) minutes, the system shall automatically blank the screen and suspend the session. Re-establishment of the session shall take place only after the user has provided the correct password. This suspension period can be shortened for administrators and users of confidential data or be lengthened for systems intended for broad use.

7.2.2.18 Users with privileged access to highly sensitive information systems should logout from the network or suspend the session manually if the computer terminal, workstation or desktop computer will be

left unattended for any period. Re-establishment of the session shall take place only after the user has provided the correct password.

7.2.3 Malware, Phishing and Virus

7.2.3.1 Malicious software including viruses and spyware pose risks to the security and confidentiality of Information. To reduce risk, AECF has put in place a number of measures to prevent these emails from reaching our Systems and operations. You may however occasionally receive a malicious email in your inbox. If it looks suspicious – do not click on it.

7.2.3.2 Phishing scams are typically fraudulent email messages appearing to come from legitimate enterprises. These messages usually direct you to another website or otherwise get you to divulge private information such as your username and password or internet banking details.

7.2.3.3 AECF Staff shall:

7.2.3.3.1 Ensure all their devices (even if it is your personal property) has anti-malware software installed. Contact the ICT Manager regarding anti-malware guidance if required.

7.2.3.3.2 Keep their personal devices that link to AECF Systems up to date with security and other vendor recommended patches.

7.2.3.3.3 Report all suspected malware or phishing mails immediately to the ICT Manager. Delete the suspected email message from your Inbox and empty it from the deleted items folder to avoid accidentally accessing the email again.

7.2.3.3.4 Think before posting on social media. Attackers will use social media as a tool to gain the trust of their targets.

7.2.3.3.5 Pay careful attention when choosing email recipients. Autofill can be the source of great risk when the wrong recipient is, inadvertently, chosen.

7.2.3.3.6 Update and run your virus scanner, firewall, and spyware checkers on your personal devices.

7.2.3.3.7 Reboot your laptop at least once a week to allow it to receive the latest security patches.

7.2.3.3.8 Ensure to follow additional guidelines if you are in part of the AECF business that has special requirements.

7.2.3.3.9 Look out for:

- **Attachments and links:** Be wary of any unexpected email attachments or links, even from people you know.
- **Senders you do not recognise:** If the sender is someone, you do not recognise the chances are the email is either spam or phishing. If the email contents look odd, hover over the email name to see the sender's address.
- **Requests for passwords or other private information:** Ignore commands and requests for action, and never send sensitive information in an email. Password-protect any confidential information that must be sent over email.

- **URLs do not match:** Hover over links in email messages to verify the actual destination, even if the link comes from a trusted source.
- **Missing lock icon or other security identifier:** Look for “https://” and a lock icon in the address bar before entering any private or sensitive information. (An easy way to remember: the “s” in “https” stands for secure.)
- **Tone and grammar:** Be suspicious of messages with grammatical or spelling errors or urgent or threatening language or tone. Certainly be skeptical of emails requesting transfer of funds or information.

7.2.3.3.10 AECF Staff shall not:

- Remove any security features from devices;
- reply to or click the links in any suspicious message;
- Email any AECF Information to personal email accounts such as Gmail, Yahoo, or other third-party Systems, unless specifically required by the AECF Management.
- Use your AECF email address as an account username for third-party sites.

8. DATA SECURITY

8.1. All Staff are responsible for ensuring that any Personal Information, which AECF holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by AECF to receive that information and has entered into a confidentiality agreement.

8.2. All Personal Information should be accessible only to those who need to use it, and access may only be granted to those authorised. Staff should form a judgment based upon the sensitivity and value of the information in question, but personal data must be kept:

8.2.1 in a lockable room with controlled access; and/or

8.2.2 in a locked drawer or filing cabinet; and/or

8.2.3 if computerised, password protected in line with corporate requirements in the access.

8.3. AECF shall ensure that all reasonable measures are taken to minimise the risk of compromising Personal Information.

8.4. It is important that AECF Staff keep all Personal Information safe and secure, whether held physically or electronically, and not disclose or allow access to unauthorised persons.

8.5. AECF will take steps to ensure that there are adequate administrative and technical measures to secure Personal Information held by AECF.

8.6. AECF’s ICT Manager will be responsible for implementing and maintaining technical measures.

8.7. AECF will also take steps as an organisation to ensure that Staff, and others to whom this Policy applies, are aware of their obligations in relation to Personal Information generally and take security precautions

to ensure data security, including the secure use of email, internet, laptops, computer hard drives, USB chips and mobile devices.

9. DATA PROCESSING

9.1. Information is not allowed to be transferred without a legitimate business purpose. Storing and sending Information to unauthorised sites is also prohibited. AECF has deployed various technologies and tools to assist in identifying and blocking of illegitimate Processing of Information, however, it remains the User's responsibility to only use approved sites.

9.2. Actions to be undertaken:

9.2.1 Make use of AECF's approved data processing tools pre-installed in the laptop as the legitimate processing tools.

9.2.2 Confidential Information of Users must always be shared and stored:

9.2.3 With authorised recipients;

9.2.4 For legitimate business purposes (i.e. contractual obligations)

9.2.5 In line with the provisions of the Applicable Regulations and other laws in the jurisdictions in which AECF operates, our contractual obligations and where applicable, EU GDPR provisions.

9.2.6 In the event that AECF Staff require to use a Software as a Service (Saas) solution or cloud hosting subscription, the staff must reach out to the AECF ICT Manager for assistance.

9.3. **DO NOT:**

9.3.1 Send AECF or its Partners' Information to your personal email addresses i.e. gmail, Hotmail, among others;

9.3.2 Use personal email address for official communication;

9.3.3 Provision any systems on private cloud hosting subscriptions using your personal or company credit card. AECF has approved subscriptions for, among others, Microsoft Office 365, Microsoft Azure, Doodle, GoDaddy & Namecheap. Other cloud hosting solutions are not allowed unless approved by AECF in writing.

9.3.4 Use WhatsApp save for informal communications, limited to publicly available information and Information that would not put AECF, our Partners, Stakeholders or Users at risk.

10. TRANSFER OF DATA TO THIRD PARTIES

In the event that AECF uses any third-party or Partner to Process Personal Information on AECF's behalf, AECF shall ensure that the respective contracts are compliant with this Policy and the Partner(s) has agreed to adopt security measures to safeguard Personal Information that is appropriate to the associated risks.

11. DATA BREACHES AND NOTIFICATION

11.1. A Data Breach includes but is not limited to the following:

11.1.1 unauthorised disclosure of Personal Information;

11.1.2 loss or theft of confidential or sensitive Data/Information;

11.1.3 loss or theft of equipment on which Personal Information is stored (e.g. loss of laptop, AECF issued external hard drive, USB stick, iPad/tablet device, or paper record);

11.1.4 unauthorised use of, access to or modification of IT, data or information systems (e.g. via a hacking attack); and

11.1.5 attempts (failed or successful) to gain unauthorised access to IT, data or information systems.

11.2. If any member of Staff, or other person learns of a suspected or actual Personal Data Breach, it must be reported to the ICT Manager immediately. The report should include as many details of the incident as possible, including date and time of the breach (if known), the nature of the information concerned, and how many individuals are involved. ICT department will perform incident management and take appropriate remedial measures in a timely manner. Staff shall report any Data Breach within 24 hours of becoming aware of such breach.

12. DESTRUCTION/RETENTION OF INFORMATION

12.1. All records whether electronic or in hard copy need to be appropriately protected. AECF Staff shall ensure records are kept securely whilst they are needed, and ensure they are destroyed promptly and in an appropriate manner when they are no longer required.

12.2. AECF adheres to a 7 year default retention period for Information- subject to instances where statutory requirements or specific business requirements impose a longer retention period.

12.3. When the retention period is reached, information shall be securely destructed.

12.4. However, records should not be destroyed without checking the legal retention period requirements with the Legal department.

12.5. AECF shall:

12.5.1 Not retain Information for any period longer than is necessary for achieving the purpose it was Processed for.

12.5.2 Ensure that the retention period is compliant with any legislative requirements.

12.5.3 Destroy records securely and in a timely manner.

12.5.4 Organise business records so that they are clearly identifiable and held in well-structured folders.

12.5.5 Sort existing records and information as well as organising new business records as they are created.

12.5.6 Not destroy records without first checking the legal retention period requirements with the Legal department.

13. DATA SUBJECT'S RIGHTS.

13.1. Data Subjects (including children) have the following rights regarding Data Processing, and the Data that is recorded about them:

13.1.1 To be informed and to know about AECF's Confidential Information and Data Protection Policy and Data Processing activities.

13.1.2 To require that any incomplete or inaccurate Information is corrected.

13.1.3 To prevent processing likely to cause damage or distress.

13.1.4 To request AECF to provide copies of Personal Information held about them in a commonly used and easily storable format.

13.1.5 To withdraw Consent at any time.

13.1.6 To be notified of the Processing of Personal Information.

13.1.7 To be informed about the mechanics of automated decision-taking process that will significantly affect them.

13.1.8 Not to have significant decisions that will affect them taken solely by automated process.

13.1.9 To sue for compensation if they suffer damage by any contravention of this Policy.

14. INFORMATION INCIDENT REPORTING

14.1. Information Incident is any incident that could potentially or that literally result in the destruction, loss, alteration, unauthorised disclosure of, or access to, Information.

14.2. Information incidents can be caused by loss/theft, insufficient control over access, equipment failure, human error, environmental causes such as fire, hacking or deception and applies to all Information Assets that contains information.

14.3. In the event AECF Staff, or Partner(s) are involved or become aware of an Information Incident or potential Information Incident, they shall, immediately, contact the ICT Manager with a copy to the legal department through the following contacts:

- Tel: +254 111 035 000
- Email: ITSupport@aecfafrica.org with a copy to legal@aecfafrica.org

14.4. AECF Staff and/or Partner(s) shall not:

14.4.1 Notify Data Subject(s) or external third party/s prior to reporting the incident as required above.

14.4.2 Delay or avoid reporting – early reporting can enable preventative measures.

15. COMMUNICATION

For additional guidance on the provisions of this Policy and/or the laws and regulations governing data protection, please contact the Head of Legal (legal@aecfafrica.org) and the ICT Manager ITSupport@aecfafrica.org

16. WHISTLEBLOWER POLICY

As a part of a comprehensive Information and Data Protection Policy initiative, The AECF has developed a Whistleblower policy. This policy is intended for all AECF staff as well as external stakeholders including: vendors, consultants, contractors and grantees. The intent of the policy is to provide a mechanism to ensure transparency and integrity in all AECF's operations through a well-defined policy that protects individuals who report known or suspected acts of fraud, misconduct, corruption or illegal activity. For further details on the Policy and mechanisms of reporting an irregularity, please contact AECF@tip-offs.com

17. EXCEPTION TO POLICY PROVISIONS

All requests for exceptions to this Policy should be documented and approved by the AECF Information Protection Officer (or equivalent as applicable).

18. REVIEWS OF POLICY

AECF reserves the right to review, re-evaluate and amend this Policy at any time.

APPENDIX 1
CLASSIFICATION, LABELLING AND HANDLING OF INFORMATION

Elements	**Public**	**Confidential**
Definitions	Information (Data) available to the public or intended for public sharing	Information (Data) not known to the public that relates to our business or that we receive in the course of business from other Stakeholders or third parties including Information of a highly regulated nature that requires a higher duty of care
	Any Information that is not classified or labelled will default to **Confidential Information** and must be handled accordingly – until classified and labelled otherwise. Information must be labeled in accordance with the Classification categories as identified by the ICT Manager.	
Data Types	AECF Information (Data)	AECF Information (Data) Stakeholder and Personal Information (Data)
Data Qualifiers	Any Information (Data) which is allowed for public consumption by the data owner.	• Intellectual property • Personal information (PI) • Sensitive Personal Data • Financial information • Competitive intelligence • Legal communication/opinions • Other (based on contractual terms, regulations)
Illustrative examples	Indefinite set of examples as indicated in the definition	1. Methodologies, deliverables, products and services information, software which may be protected using trade secrets, trademarks, copyright, and patents, policies, standards, procedures (e.g. firewall rules, infrastructure manuals, etc.), account numbers,

		address, date of birth, personnel number, photograph, video identifiable to an individual, financial or salary data, products, markets, pricing, business plans, usage rates, pricing, sales pipeline, marketing data and other internal (non-sensitive and non-public) data. 2. Data on medical or health conditions, racial or ethnic origin, political opinions, religious, or philosophical beliefs, sexual preferences, data related to offenses or criminal convictions, government identifiers, financial account numbers, and passwords or personal identification numbers for financial accounts, forensic investigation data, fraud investigation data, Mergers & Acquisitions (M&A), restructuring or bankruptcy, legal and other sensitive matters.
Risks	Low	1. Medium 2. High