Data Protection Policy

Document Version:	1	Date:	May 2018

Document History

Version	Summary of Amendment	Author	Date

Table of Contents

---

1. Introduction

1.1 Ape Action Africa, regards the lawful and correct processing of personal and sensitive data as an integral part of its purpose and vital for maintaining confidence between employees, clients, visitors, members and other stakeholders whom we process data about, on behalf of and ourselves.

2. Policy Statement

2.1 This Data Protection Policy explains how Ape Action Africa will meet its legal obligations concerning confidentiality and data security standards. The requirements within the policy are primarily based upon the Data Protection Act 1998 and EU General Data Protection Regulation (GDPR) – from 25th May 2018 - which are the key pieces of legislation covering data security and confidentiality of personal and sensitive personal data.

- Ape Action Africa will fully implement all aspects of UK data protection legislation
- Ape Action Africa will ensure all employees and others handling personal data are aware of their obligations and rights under UK data protection legislation.
- Ape Action Africa will implement adequate and appropriate physical, technical and organisational measures to ensure the security of all data contained in or handled by those systems.

2.2 The main focus of this policy is to provide guidance about the protection, sharing and disclosure of employee, visitor, member and client data, but it is important to stress that maintaining confidentiality and adhering to data protection legislation applies to anyone handling personal data or personal sensitive data on behalf of Ape Action Africa.

3. Registration with the Information Commissioner

3.1 UK data protection legislation requires data controllers (e.g. organisations) to register with the Information Commissioner (ICO) the categories of data they hold about people, and what they do with it.

3.2 Ape Action Africa is registered with the ICO. This is continually reviewed by the data protection officer and any requirement to amend our registration must be actioned promptly.

4. Definition of Personal Data and Sensitive Personal Data

- All identifiable data of an individual
- All identifiable employee data
- All identifiable client, visitor and member data
- All identifiable data including that of students
- All other personal data processed by Ape Action Africa

4.1 Examples of personal identifiable data Ape Action Africa processes include:

- Names, addresses, emails, phone numbers and other Ape Action Africa information;
- Financial information;
- National insurance numbers and payroll data;
- Information about someone's health;
- Member / Client data
- CCTV footage
- All data within Ape Action Africa
- Photographs, video and audio recordings.

4.2 Certain types of data is regarded as sensitive and attracts additional legal protection. Sensitive personal data is considered to be any data that could identify a person such as:

- Details of bank account, national insurance number, any ID details such as passport or driving license, etc.
- The racial or ethnic origin of the data subject;
- Political opinions;
- Religious beliefs or other beliefs of a similar nature;
- Membership of a trade union;
- Physical or mental health or condition;
- Sexual orientation and lifestyle;
- Commission or alleged commission of any offence;
- Any proceeding for any offence committed or alleged to have been committed or disposal of such proceedings or the sentence of court in such proceedings;

5. Data Protection Principles

5.1 The Data Protection principles that lie at the heart of the data protection legislation give the data protection legislation its strength and purpose. To this end, Ape Action Africa fully endorses and abides by the principles of data protection. Specifically, the eight principles require that:

- **Principle 1: Fair and Lawful -** Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met. See 'The 'Conditions of Processing' guidance.
- **Principle 2: Purpose -** Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
- **Principle 3: Adequacy -** Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- **Principle 4: Accuracy -** Personal data shall be accurate and where necessary kept up to date.
- **Principle 5: Retention -** Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- **Principle 6: Rights -** Personal data shall be processed in accordance with the rights of data subjects under this Act.
- **Principle 7: Security -** Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- **Principle 8: International -** Personal data shall not be transferred to a country or territory outside the European Economic Area (EEA) (which includes all EU countries and in addition, non-EU countries Iceland, Liechtenstein and Norway) or Switzerland unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

5.2 Personal data and sensitive personal data (also known as special category data) must not be used other than for specific purposes required to deliver a product or service. The data subject should always know that their data is being processed. When that data is sensitive, for example health information, consent is required before the data can be processed by Ape Action Africa.

5.3 All data collected from young people under the age of 16, unless there are concerns about mental capacity in which case this should be extended, is to be treated as sensitive personal data.

5.4 A record can be in computerised and/or manual form. It may include such documentation as:

- Manually stored paper data e.g. employee records
- Hand written notes.
- Letters to and from Ape Action Africa.
- Electronic records.
- Printouts.
- Photographs.
- Videos and tape recordings.

5.5 Backup data (i.e. archived data or disaster recovery records) also falls under the data protection legislation; however, a search within them should only be conducted if specifically asked for by the data subject.

6. Rights of Access by Individuals

The data protection legislation gives every living person (or their authorised representative) the right to apply for access to the personal data which organisations (data controllers) hold about them irrespective of when and how they were compiled, i.e. hand written records, electronic and manual

records held in a structured file, subject to certain exemptions. This is called a Subject Access Request. The data protection legislation treats personnel data relating to employees and clients alike.

7. Practical Implications

7.1 Understanding and complying with the principles is the key to understanding and complying with our responsibilities as a data controller. Therefore, Ape Action Africa will, through appropriate management, and strict application of criteria and controls:

- Ensure that there is a lawful ground for using the personal data.
- Ensure that the use of the data is fair and that will meet one of the specified conditions.
- Always make sure the data subject has been issued with a clear fair processing notice describing how we will use their data.
- Only use sensitive personal data where Ape Action Africahas obtained the individual's explicit consent; unless an exemption applies.
- Only use sensitive personal data, if it is absolutely necessary for Ape Action Africato use it.
- Explain to individuals, at the time their personal data is collected, how that information will be used.
- Only obtain and use personal data for those purposes which are known to the individual.
- Personal data should only be used for the purpose it was given. If we need to use the data for other purposes, further consent may be needed.
- Only keep personal data that is relevant to Ape Action Africa.
- Keep personal data accurate and up to date.
- Only keep personal data for as long as is necessary.
- Always adhere to our Subject Access Request Procedure and be receptive to any queries, requests or complaints made by individuals in connection with their personal data.
- Always allow individuals to opt-out of receiving bulk information with exception of core administrative emails such as renewals. Ape Action Africa will always suppress the details of individuals who have opted out of receiving information (e.g. marketing).
- Will always give an option to "opt in" when consent is needed to share personal data unless there is a statutory/ legal reason to do so.
- Take appropriate technical and organisational security measures to safeguard personal data.

7.2 In addition, Ape Action Africa will ensure that:

- There is an employee appointed as the Data Protection Officer with specific responsibility for Data Protection in Ape Action Africa (see below for roles and responsibilities).
- Everyone managing and handling personal data and sensitive personal data understands that they are legally responsible for following good data protection practice and has read and signed the data protection policy.
- Everyone managing and handling personal data and sensitive personal data is appropriately supervised by their line manager.
- Enquiries about handling personal data and sensitive personal data are promptly and courteously dealt with.
- Methods of handling personal data and sensitive personal data are clearly described in polices and guidance;
- A review and audit of data protection arrangements is undertaken annually
- Methods of handling personal data and sensitive personal data are regularly assessed and evaluated by the Data Protection Officer and relevant directors.

- Performance with personal data and sensitive personal data handling is regularly assessed and evaluated by the Data Protection Officer and relevant directors.
- Formal written Data Processing Agreements are in place before any personal data and sensitive personal data is transferred to a third party.

8. Roles and Responsibilities

8.1 Maintaining confidentiality and adhering to data protection legislation applies to everyone at Ape Action Africa. Ape Action Africa will take necessary steps to ensure that everyone managing and processing personal data understands that they are responsible for following good data protection practice. Employees will receive training and sign the policy every twelve months as part of their induction.

8.2 All Employees have a responsibility to:

- Observe all guidance and codes of conduct in relation to obtaining, using and disclosing personal data and sensitive personal data ;
- Obtain and processing personal data and sensitive personal data only for specified purposes;
- Only access personal data and sensitive personal data that is specifically required to carry out their activity or work;
- Record data correctly in both manual and electronic records;
- Ensure any personal data and sensitive personal data is held is kept secure;
- Ensure that personal data and sensitive personal data is not disclosed in any form to any unauthorised third party;
- Ensure personal data and sensitive personal data is sent securely; and
- Read and sign the policy, raising any questions to check understanding.

8.3 Failure to adhere to any guidance in this policy could mean an individual(s) being criminally liable for deliberate unlawful disclosure under the data protection legislation. This may result in criminal prosecution and/or disciplinary action.

8.4 All Managers are responsible for:

- Determining if their operational area holds personal data and sensitive personal data and ensuring that the data is adequately secure, access is controlled and that the data is only used for the intended purposes(s);
- Provide clear messaging to those in their teams about data protection requirements and measures;
- Ensure personal and sensitive personal data is only held for the purpose intended;
- Ensure personal and sensitive personal data is not communicated or shared for non authorised purposes; and
- Ensure personal and sensitive personal data is encrypted when transmitted or appropriate security measures are taken to protect when in transit or storage.

8.5 Data Protection Officer – The Director is appointed as the Data Protection Officer. Responsibilities include:

- Ensuring compliance with legislation principles;
- Progressing the Data Protection Action Plan;

- Ensuring notification of processing of personal data and sensitive personal data to the Information Commissioner is up to date;
- Providing guidance and advice to employees in relation to compliance with legislative requirements;
- Auditing data protection arrangements annually;
- Reporting on any breaches of Data Protection legislation;
- In the Data Protection Officer's absence, advice can be gained from http://www.ico.gov.uk/; and
- Ensuring those handling personal data are aware of their obligations by producing relevant policy, auditing the arrangements and ensuring relevant people receive training.

8.6 Responsibility of the Director at Ape Action Africa has overall responsibility for Data Protection within Ape Action Africa. Ape Action Africa has a duty to ensure that the requirements of the data protection legislation are upheld.

8.7 The Information Commissioner Office (ICO) – The Information Commissioner's Office is responsible for overseeing compliance e.g. investigating complaints, issuing codes of practice and guidance, maintaining a register of data protection officers. Any failure to comply with data protection legislation may lead to investigation by the ICO which could result in serious financial or other consequences for Ape Action Africa and/or its members.

9. Breach of Policy

9.1 In the event that an employee fails to comply with this policy, the matter may be considered as misconduct and dealt with in accordance with Ape Action Africa Disciplinary Policy and procedure.

10. Dealing with a Data Breach

10.1 If a data breach is suspected, the person who identified the breach should immediately:

- Notify the relevant department manager and
- Notify the Data Protection Officer
- Complete and return a breach report available from the Data Protection Officer and also located on Ape Action Africa's shared drive.

10.2 Following notification of a breach, the Data Protection Officer will take the following actions as a matter of urgency:

- Assess the risks associated with the breach;
- Implement a recovery plan, including damage limitation;
- Inform the appropriate people and organisations that the breach has occurred;
- Notify the client if client data has been breached
- Review our response and update our information security.

11. Policies and Procedures

11.1 This policy should be read in conjunction with the following policies and guidance:

- Record Retention and Management Policy
- How to encrypt and open encrypted documents
- Dealing with a Data Subject Access Request
- Fair Processing Notices (as relevant to Data Subject catergory)

12. Glossary of Terms

Data Subject
Means an individual who is the subject of personal data or sensitive personal data. This includes an employee, client or other identifiable individual.

Data Controller
Means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data and sensitive personal data are, or are to be processed.

The data controller is Ape Action Africa for employee data. The client is the data controller of their employee data

Data Processor
In relation to personal data or sensitive personal data, means any person who processes that data on behalf of the data controller but it is not employed by them. Ape Action Africa is a data processor in respect of client data.

Third Party
In relation to personal data or sensitive personal data, means any person other than the data subject, the data controller, or any data processor or other person authorised to process data for data controller or processor. For example, the police or HMRC.

Processing
Means recording or holding data or carrying out any operations on that data; including organising, altering or adapting it; disclosing the data or aligning, combining, blocking or erasing it. Essentially if you have it, you are processing it.

Data Breach
Is a failure leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or sensitive personal data.

Subject Access Request
This is a written, signed request (which includes emails and other written formats) from an individual to see data held on them. The Data Controller must provide all such information in a readable form within 40 days of receipt of the request and will charge a fee of £10. **From 25th May 2018 requests must be dealt with in 30 days and the £10 fee will no longer apply.**

This policy is subject to change by Ape Action Africa, in line with changes in statutory law, case law and best practice. It does not form part of an employee's Contract of Employment.