1. Introduction

1.1. AngloGold Ashanti (AGA) has operations in various countries globally where data protection laws can vary. AGA has identified the core values, policies and standards to achieve broad compliance with relevant legislation and they are set out in this Policy. This Policy will be supplemented with alternative or additional requirements applicable to individual countries.

1.2. In this Policy the following definitions have the following meanings:

1.2.1. **Personal data** means any information likely to come into AGA’s possession that is related to and identifies an individual, either on its own or together with other information that the company may receive.

1.2.2. **Employees** refer to full time employee, part time employee, fixed-term full time, fixed-term part time, contractors, director, casual/temporary, GEC employee, pensioner, expats and trainee/learner and includes applicants for such positions.

2. Policy & Purpose

This Policy confirms AGA’s commitment to compliance with the requirements of data protection laws and regulations applicable to AGA in the countries in which it, or a third party supplier on its behalf, processes personal data.

3. Applicability

This Policy applies to all AGA employees and all third-party suppliers who receive or have access to personal data from AGA or who provide information to AGA, regardless of geographic location.

4. Principles

4.1. AGA will ensure that privacy and data protection compliance standards be adhered to across all employee management systems and processes.

4.2. AGA has adopted the following principles to govern its processing of personal data (except as specifically provided by this Policy or as required by the applicable laws):

4.2.1. Personal data will be processed fairly and lawfully;
4.2.2. Personal data will be obtained only for specified and lawful purposes and will not be further processed in any way that is considered incompatible with those purposes;

4.2.3. Personal data will be adequate, relevant and not excessive in relation to the purposes for which it is processed;

4.2.4. Personal data will be accurate, complete and current as appropriate to the purposes for which it is collected and/or processed as far as is reasonably practical;

4.2.5. Personal data shall not be kept in a format which allows for the identification of the employee for longer than necessary for the specified purpose;

4.2.6. Personal data shall not be collected or processed unless:

4.2.6.1. The employee has provided a valid, informed consent where required;
4.2.6.2. Processing is necessary for the fulfilment of the employment relationship;
4.2.6.3. Processing is necessary for compliance with an AGA legal obligation;
4.2.6.4. Processing is necessary in order to protect the employee’s interests;
4.2.6.5. Processing is necessary for the performance of a public interest activity;
4.2.6.6. Personal data shall be collected and processed in accordance with the rights of the employee.

4.2.7. Appropriate measures shall be taken to:

4.2.7.1. Prevent and/or to identify unauthorised or unlawful collection, processing, transmittal of personal data; and
4.2.7.2. Prevent accidental loss or destruction of, or damage to personal data.

5. Standard

5.1. Employee Consent

5.1.1. AGA will ensure a system for the collection and documentation of employee consent for the processing and transfer of personal data.

5.1.2. Consent with respect to sensitive data shall refer expressly to the data being processed. Sensitive data includes race/ethnic origin, union membership, health information and criminal convictions.

5.2. Transfer of Personal Data

5.2.1. Personal data shall not be transferred to another entity or country unless reasonable steps have been taken to maintain the required level of data protection (being the same or better than the current level of protection offered).
5.2.2. Personal data may be communicated to third persons only for the purpose for which it was originally collected or for other legal purposes.

5.2.3. All transfers to third parties shall be subject to written agreements setting out clear obligations on the third party to provide the same level of protection to the personal data as offered by AGA.

5.2.4. Notwithstanding the above, personal data may only be transferred where any of the following apply:

5.2.4.1. The employee has given prior written consent to the proposed transfer;
5.2.4.2. The transfer is necessary for the fulfilment of the relationship between the employee and AGA;
5.2.4.3. The transfer is required by law; or
5.2.4.4. The transfer is necessary in order to protect the employee’s vital interests.

5.3. Employee Access Rights

5.3.1. AGA shall establish a system to enable and facilitate employee access rights to their personal data.

5.3.2. Employees shall be entitled to obtain the following information about their own personal data upon a request made in compliance with the specific procedure established:

5.3.2.1. Whether AGA has stored personal data regarding them;
5.3.2.2. Access to personal data stored concerning them;
5.3.2.3. The sources through which the personal data was obtained;
5.3.2.4. Whether any data held on them is sensitive data;
5.3.2.5. The purpose that motivated the collection of the personal data;
5.3.2.6. The recipients of the collected personal data;
5.3.2.7. How corrections will be made if the data held is incorrect;
5.3.2.8. That personal data held on them be kept up-to-date;
5.3.2.9. The removal of their personal data where factually inaccurate;
5.3.2.10. The confidential treatment of their personal data;
5.3.2.11. A copy of the consent given to AGA by the employee allowing the processing of their personal data; and
5.3.2.12. The withdrawal of consent given that allows the processing of their personal data.

5.3.3. AGA shall provide its response to a request under section 5.3.2 within ten (10) days of receipt of the request.

5.3.4. Where the request concerns the update, removal and/or confidential treatment of their personal data, AGA shall provide its response within five (5) days of receipt of such a request.

5.3.5. During the process of reviewing, correcting or verifying any personal data, AGA will ensure that the file containing such data is either blocked or is clearly stated as being under review.
6. Notification

AGA shall not process personal data without notification to the relevant data protection authorities in countries which require such notification.

7. Third Party Processors

7.1. Where AGA relies on others to assist in its processing activities, AGA will choose a data processor that provides sufficient security measures and takes reasonable steps to ensure compliance with those measures.

7.2. AGA shall enter into written contracts with each data processor requiring it to comply with data privacy and security requirements imposed on AGA by law and with this Policy.

7.3. As part of AGA's internal data auditing process, AGA shall conduct regular checks on processing by third party processors, especially in respect of security measures.

8. Security

AGA shall adopt physical, technical, and organizational measures to ensure the security of personal data, including the prevention of their alteration, loss, damage, unauthorized processing or access, having regard to the state of the art, the nature of the data, and the risks to which they are exposed by virtue of human action or the physical or natural environment.

9. Retention

All employees must observe the AGA data retention policy. AGA will delete personal data after a reasonable time and will ensure that it does not keep personal data for longer than is necessary for the purpose for which it is being held except where it is necessary to keep it indefinitely or the law requires it be kept for a certain time. When AGA no longer needs to keep such personal data it will destroy it as soon as reasonably practicable.