APPROVED CORPORATE POLICY

Data Protection and Privacy Policy

How Chwezi Core Systems collects, uses, stores, shares and protects personal data, and how individuals exercise their rights under the Data Protection and Privacy Act, 2019 of Uganda.

DOCUMENT ID	CCS-POL-DPP-02
VERSION	1.0
STATUS	APPROVED
CLASSIFICATION	Public
POLICY OWNER	Data Protection Officer
APPROVED BY	Peter Bamuhigire, Founder and Chief Technology Officer
APPROVAL DATE	27 October 2026
EFFECTIVE DATE	1 November 2026
NEXT REVIEW	October 2027

Peter Bamuhigire
Founder and Chief Technology Officer
For and on behalf of Chwezi Core Systems Limited

27 October 2026
Date of approval
Effective 1 November 2026

Contents

1. Purpose
2. Scope
3. Summary in plain language
4. Definitions
5. Our role: controller and processor
6. Data protection principles
7. Personal data we process as controller
8. Lawful basis, consent, children and special personal data
9. Data we process for clients
10. Where data is stored: transfers outside Uganda
11. Sharing and sub-processors
12. Security of personal data
13. Retention and disposal
14. Rights of data subjects
15. Personal data breaches
16. Websites, cookies and analytics
17. Direct marketing
18. Privacy by design and impact assessments
19. Roles and responsibilities
20. Training, monitoring and breach of policy
21. Complaints and the regulator
22. Contact
23. Review and approval history

1. Purpose

This policy sets out how Chwezi Core Systems Limited ("Chwezi", "we") collects, uses, stores, shares and disposes of personal data, and how individuals can exercise their rights over it. It also sets the duties Chwezi accepts when it processes personal data on behalf of clients in the software we build and host.

2. Scope

This policy applies to all personal data Chwezi processes, in any form, about:

- visitors to our websites and people who send us enquiries;
- clients' contact persons and prospective clients;
- users of the software products we host (including Kraal Code, Maduuka and Aqar) and the people whose records our clients keep in them;
- job applicants, staff, interns and contractors;
- suppliers' contact persons.

It applies to every director, employee, intern, contractor and consultant who works for Chwezi ("personnel"), and to suppliers who process personal data for us.

3. Summary in plain language

- We collect only the personal data we need to answer you, deliver our services, employ our people and meet the law.
- We do not sell personal data, and we do not use it for third-party advertising.
- Some of our systems and websites are hosted on servers in the United States of America, Finland and Germany. We protect data in those locations with encryption, access controls and contracts with our hosting providers.
- When a client keeps its records in software we host, the client decides how that data is used; we follow the client's instructions and keep the data secure.
- You can ask to see, correct or delete your personal data, or object to its use, by writing to info@chwezicore.com. We reply within 30 days.
- Chwezi is registered with the Personal Data Protection Office, Uganda's data protection regulator.
- If you are not satisfied, you can complain to the Personal Data Protection Office in Uganda.

4. Definitions

Term	Meaning
Personal data	Information about an identified or identifiable living person, as defined in the Data Protection and Privacy Act, 2019 of Uganda.

Term	Meaning
Special personal data	Personal data revealing religious or philosophical beliefs, political opinions, sexual life, financial information, health status or medical records, as set out in the Act.
Data subject	The person the personal data is about.
Data controller	The person or organisation that decides why and how personal data is processed.
Data processor	A person or organisation that processes personal data on behalf of a data controller.
Processing	Any operation on personal data, including collecting, recording, storing, using, sharing, transferring and deleting it.
Personal data breach	A breach of security leading to the accidental or unlawful loss, destruction, alteration, disclosure of, or access to, personal data.
Sub-processor	A supplier Chwezi engages to process client personal data, such as a hosting provider.
PDPO	The Personal Data Protection Office, Uganda's data protection regulator, established under the Act within the National Information Technology Authority – Uganda.
Data Protection Officer	The person accountable for this policy. Until another person is designated in writing, this is the Founder and Chief Technology Officer.

5. Our role: controller and processor

5.1 **Chwezi as controller.** Chwezi is the data controller for personal data it collects for its own purposes: website enquiries, client and supplier contacts, marketing, recruitment and employment.

5.2 **Chwezi as processor.** When a client stores personal data in a system Chwezi builds, hosts or supports, the client is the data controller and Chwezi is the data processor. In that role Chwezi must:

- process the data only on the client's documented instructions, as set out in the contract and the configuration the client chooses;
- not use client data for its own purposes, including marketing or product analytics that identify individuals;
- bind every person who has access to the data to confidentiality;
- apply the security controls in the Information Security Policy (CCS-POL-ISP-01);
- engage sub-processors only as set out in section 11;
- help the client respond to data subject requests and meet its own breach notification and impact assessment duties;
- at the end of the service, return the client's data in a usable export format and then delete it, unless the law requires it to be kept;
- give the client the information it reasonably needs to show compliance, and allow audits agreed in the contract.

5.3 Where a client's law sets duties for processors beyond those in this policy, such as the Kenya Data Protection Act, 2019 or the EU General Data Protection Regulation, Chwezi must meet those duties for that client when the contract requires it.

6. Data protection principles

Chwezi must process personal data in line with the principles of the Data Protection and Privacy Act, 2019. In practice this means personal data must be:

1. processed lawfully, fairly and transparently;
2. collected for a specific, explicit and lawful purpose and not used in a way incompatible with that purpose;
3. adequate, relevant and limited to what the purpose needs;
4. accurate and kept up to date;
5. kept no longer than the purpose or the law requires;
6. protected by appropriate security;
7. processed in a way that respects the rights of data subjects;
8. transferred outside Uganda only as section 10 allows.

7. Personal data we process as controller

Who	What data	Why	Basis	How long we keep it
Website visitors and enquirers	Name, organisation, email, phone, message content	To answer the enquiry and prepare proposals	Consent, given by submitting the enquiry (s.7(1))	24 months after the last contact, unless it becomes a client relationship
Client and prospective client contacts	Name, job title, organisation, email, phone, communication history	To deliver, invoice and support services; to manage the relationship	Performance of a contract, or steps requested before one (s.7(2)(c))	Contract period plus the period required by tax and company law
Users of hosted software (account data)	Name, email, phone, role, sign-in records, audit-trail entries	To provide secure access and support, and to keep security logs	Performance of the client contract (s.7(2)(c)); compliance with legal obligations (s.7(2)(e))	Life of the user account plus 12 months for security logs
Job applicants	CV, contact details, qualifications, references, interview notes	To assess applications	Steps taken at the applicant's request before a contract (s.7(2)(c)); consent to keep a CV for future roles	12 months after the recruitment closes, unless the applicant is hired
Staff, interns and contractors	Identity and contact details, contract, bank and tax details, payroll, performance, emergency contacts	To employ or engage the person and meet employment and tax law	Contract (s.7(2)(c)); legal obligation (s.7(2)(e))	Engagement period plus the period required by employment and tax law
Supplier contacts	Name, organisation, email, phone, payment details	To buy and pay for goods and services	Contract (s.7(2)(c)); legal obligation (s.7(2)(e))	Contract period plus the period required by tax and company law

Who	What data	Why	Basis	How long we keep it
Marketing contacts	Name, email, organisation, preferences	To send news and insights the person has asked for	Consent (s.7(1))	Until consent is withdrawn

8. Lawful basis, consent, children and special personal data

8.1 Personnel must not collect or process personal data without the prior consent of the data subject, unless section 7(2) of the Act permits it: where the processing is authorised or required by law, is necessary for the performance of a contract with the data subject or for steps the data subject has asked for before a contract, is for medical purposes, or is needed to comply with a legal obligation. Chwezi does not rely on a "legitimate interests" ground, because the Act does not provide one.

8.2 Where a data subject objects to processing that rests only on consent, Chwezi must stop that processing, as section 7(3) of the Act requires.

8.3 Where Chwezi relies on consent, the consent must be informed, specific and recorded. A data subject may withdraw consent at any time, and withdrawal must be as easy as giving it.

8.4 When collecting personal data directly from a person, Chwezi must tell them who we are, why we need the data, whether providing it is voluntary or required, who will receive it and how to exercise their rights. This policy and the privacy notice on our website provide that information.

8.5 Chwezi does not knowingly collect personal data directly from children on its own websites. Section 8 of the Act allows children's data to be processed only with the prior consent of a parent or guardian, where the law requires it, or for research or statistical purposes. Where a client's system holds children's records, for example in school or health software, the client as controller must establish that basis, and Chwezi must apply Restricted handling to those records.

8.6 Special personal data, including health and financial information held in client systems, must be handled as Restricted information under the Information Security Policy and processed only where section 9 of the Act permits it, such as with the data subject's freely given consent or to meet an employer's legal obligations.

9. Data we process for clients

9.1 Before a client system goes live, the project manager must agree with the client: the categories of personal data the system will hold, the hosting location, the users who will have access, the retention rules the client wants, and the client's contact for data protection matters.

9.2 Chwezi personnel may access client production data only to provide support, fix faults, run migrations or meet a legal obligation, and only with the minimum access needed. Such access must be logged.

9.3 Data migration files received from clients must be stored encrypted, used only for the migration and deleted within 30 days after the client signs off the migration, unless the client asks for them to be returned.

10. Where data is stored: transfers outside Uganda

10.1 Chwezi hosts some of its systems and websites on servers located in the **United States of America, Finland and Germany**. Personal data held in those systems is therefore stored and processed outside Uganda. Chwezi staff working from Uganda and other countries may also access the data remotely to provide support.

10.2 Under section 19 of the Data Protection and Privacy Act, 2019, personal data may be processed or stored outside Uganda only where the country of storage has adequate measures for protecting personal data at least equivalent to those in Uganda, or where the data subject has consented. Chwezi meets this requirement as follows:

- **Finland and Germany** are members of the European Union, where the EU General Data Protection Regulation sets a level of protection at least equivalent to Ugandan law.
- **United States of America:** Chwezi uses hosting providers that are bound by contract to keep the data confidential, to process it only to provide the hosting service, and to apply security controls certified or independently audited against recognised standards. Because these contractual and technical measures do not by themselves establish that the country's protection is equivalent to Uganda's, Chwezi relies on the data subject's consent for personal data it controls and stores there, and this policy and our website privacy notice disclose that location before the data is collected. For client data, Chwezi must agree the hosting location with the client before go-live, so that the client, as controller, can secure the basis it needs; a client may require its data to be hosted in Finland or Germany instead.
- **For all locations:** Chwezi encrypts personal data in transit and at rest, limits administrative access to named Chwezi personnel, and restricts the hosting provider's access to the content of client databases to what is needed to run the infrastructure.

10.3 Chwezi must tell each client, before go-live and on request, which country hosts that client's data.

10.4 Where a client's contract requires data to remain in a particular country or region, Chwezi must host it there and must not transfer it elsewhere without the client's written agreement.

10.5 The Data Protection Officer must review the transfer safeguards whenever a new hosting country or provider is introduced, and at each annual review of this policy.

11. Sharing and sub-processors

11.1 Chwezi does not sell, rent or trade personal data.

11.2 Chwezi may share personal data only:

- with suppliers that process it on our behalf, such as hosting, email and backup providers, under written contracts that require confidentiality and security;
- with professional advisers, such as auditors and lawyers, who are bound by confidentiality;
- with authorities where the law requires it, after checking the request is lawful;
- with the data subject's consent, or on a client's documented instruction.

11.3 Chwezi must keep a list of the sub-processors used for hosted products and their processing locations, and give it to a client on request. Chwezi must inform affected clients before adding or replacing a sub-processor that stores client data, so that they can object under the terms of their contract.

12. Security of personal data

12.1 Chwezi protects personal data with the controls in the Information Security Policy (CCS-POL-ISP-01), including access on a need-to-know basis, multi-factor authentication for administrative access, encryption in transit and at rest, daily encrypted backups, logging and monitoring, annual penetration testing of hosted products, staff confidentiality agreements and annual training.

12.2 Personnel must not copy personal data to personal devices, personal email or personal cloud accounts, or into public artificial-intelligence tools.

13. Retention and disposal

13.1 Personal data must be kept only for the periods set out in section 7, or for the period a client sets for its own data, or longer only where the law requires.

13.2 At the end of the retention period, personal data must be securely deleted or anonymised. Paper records must be shredded. Deletion from backups takes effect when the backup cycle expires.

13.3 The Data Protection Officer must check at least once a year that data past its retention period has been deleted.

14. Rights of data subjects

14.1 Under the Data Protection and Privacy Act, 2019, a data subject has the right to:

- be told what personal data we hold about them and to obtain a copy;
- have inaccurate or incomplete data corrected;
- have data deleted where it is no longer needed or was processed unlawfully;
- object to processing, including processing for direct marketing;
- withdraw consent where we rely on consent;
- not be subject to a decision based solely on automated processing that significantly affects them;
- complain to the Personal Data Protection Office.

These rights are set out in sections 24 to 28 of the Act.

14.2 Requests must be sent to info@chwezicore.com with the subject line "Data Protection Request", or delivered in writing to our office in Kampala. Chwezi may ask for proof of identity before acting on a request.

14.3 The Data Protection Officer must acknowledge each request within 5 working days and respond in full within 30 days of receiving it, as section 24(9) of the Act requires for access requests, or within any shorter period the law requires. Chwezi must not charge for a request unless it is manifestly unfounded or excessive.

14.4 Where a request concerns data a client controls, Chwezi must pass it to the client within 5 working days and help the client respond.

14.5 Where Chwezi refuses a request, it must explain why in writing and tell the person how to complain to the PDPO.

15. Personal data breaches

15.1 Every person must report a suspected personal data breach to the Data Protection Officer immediately, using the incident reporting route in section 20 of the Information Security Policy (CCS-POL-ISP-01).

15.2 The Data Protection Officer must assess the breach, record it in the breach register, and take steps to contain it and limit harm.

15.3 Section 23 of the Act applies to data collectors, processors and controllers alike. Whenever Chwezi believes that personal data has been accessed or acquired by an unauthorised person, the Data Protection Officer must immediately notify the Personal Data Protection Office, in the manner prescribed by regulation 33 of the Data Protection and Privacy Regulations, 2021, describing the unauthorised access and the remedial action taken.

15.4 Chwezi must notify affected data subjects when, and in the manner, the PDPO determines under section 23(2) and (3) of the Act: by registered mail, email, a prominent notice on our website or publication in the mass media, with enough information for them to protect themselves.

15.5 Where the breach affects data Chwezi processes for a client, Chwezi must also notify the client's designated contact without undue delay, and in any event within 72 hours of becoming aware of it, unless the contract sets a shorter period, and must coordinate the PDPO notification with the client and give the client the information it needs to meet its own duties.

15.6 Chwezi must keep a record of every personal data breach, including those not notified, with the facts, effects and corrective actions.

16. Websites, cookies and analytics

16.1 Chwezi websites must use only cookies that are needed for the site to work, unless visitors are told and, where the law requires, have given consent.

16.2 Website analytics must be configured to avoid collecting more personal data than needed, and must not be used to build advertising profiles.

16.3 Our website privacy notice, published at chwezicore.com, gives visitors the specific information about our website processing and links to this policy.

17. Direct marketing

17.1 Chwezi must send electronic marketing only to people who have consented to it or who are existing clients receiving information about similar services, and every message must include a simple way to unsubscribe.

17.2 Unsubscribe requests must be acted on within 10 working days.

18. Privacy by design and impact assessments

18.1 Every new system, product feature or service that processes personal data must be designed so that, by default, it collects the minimum data, restricts access by role and supports the retention, export and deletion of records.

18.2 Before launching a product, feature or process likely to create a high risk to individuals, such as large-scale processing of health, financial or children's data, Chwezi must carry out and record a data protection impact assessment, or support the client in carrying out its own.

19. Roles and responsibilities

Role	Responsibilities
Founder and Chief Technology Officer	Approves this policy; provides resources; holds the Data Protection Officer role until another person is designated in writing.
Data Protection Officer	Owns this policy; keeps the record of processing activities, sub-processor list and breach register; handles data subject requests and PDPO notifications; maintains Chwezi's registration with the PDPO; advises on impact assessments; arranges training.
Information Security Lead	Operates the security controls that protect personal data (CCS-POL-ISP-01); leads technical incident response.
Project and engagement managers	Agree data protection terms and hosting location with clients; make sure projects apply privacy by design.
All personnel	Process personal data only as their role requires and as this policy permits; report breaches and data subject requests immediately.

20. Training, monitoring and breach of policy

20.1 Every staff member and contractor who handles personal data must complete data protection training within their first month and at least once a year.

20.2 The Data Protection Officer must report to the Founder and Chief Technology Officer at least every six months on data subject requests, breaches, retention checks and changes in law.

20.3 The Data Protection Officer must keep the record of processing activities, consent records, data subject requests and responses, the breach register, impact assessments and the sub-processor list for at least three years after each record is closed.

20.4 A breach of this policy by personnel may lead to disciplinary action up to dismissal, or termination of a contract. The Data Protection Officer investigates; the Founder and Chief Technology Officer decides on the outcome.

21. Complaints and the regulator

21.1 Anyone who is concerned about how Chwezi handles their personal data may first contact us at info@chwezicore.com so that we can try to resolve it.

21.2 Every person also has the right to complain to the Personal Data Protection Office, Uganda (www.pdpo.go.ug).

21.3 Chwezi is registered with the PDPO in the data protection register kept under section 29 of the Act and the Data Protection and Privacy Regulations, 2021. The Data Protection Officer must keep that registration current, and must renew or update it whenever the regulations require.

22. Contact

Data Protection Officer, Chwezi Core Systems Limited
Kampala, Uganda
Email: info@chwezicore.com (subject line: "Data Protection Request")
Phone: +256 784 464178
Company registration number: 80034847127066

23. Review and approval history

Version	Date	Author	Approved by	Change	Next review
1.0	27 October 2026	Data Protection Officer	Peter Bamuhigire, Founder and Chief Technology Officer	First approved issue	October 2027

This policy must be reviewed at least once a year, and earlier after a significant breach, a change in the law or a change in where or how we host data.

Approved for and on behalf of Chwezi Core Systems Limited
Peter Bamuhigire, Founder and Chief Technology Officer — 27 October 2026