

# PRIVACY POLICY

## Zimbabwe Centre for High-Performance Computing (ZCHPC)

*How ZCHPC collects, uses, hosts, secures and shares personal data*

|                         |                                                        |
|-------------------------|--------------------------------------------------------|
| Document Owner          | DPO Department                                         |
| Approved By             | [ Committee Chairperson]                               |
| Policy Version          | V2.0                                                   |
| Classification          | Public                                                 |
| Effective Date / Review | Effective: [September 2026]   Review: [September 2027] |

**Privacy commitment:** ZCHPC is committed to lawful, fair and transparent processing, data minimisation, purpose limitation, accuracy, security, accountability and respect for the rights of individuals.

### 1. Purpose and status of this policy

This Privacy Policy explains how the Zimbabwe Centre for High Performance Computing (ZCHPC) handles personal data in the course of operating national high-performance computing, data-centre, cloud, hosting, research-support, training and related digital infrastructure services. It applies alongside customer contracts, research protocols, consent forms, acceptable-use requirements, employment policies and any service-specific privacy notices.

The policy is intended for customers, researchers, partner institutions, website users, suppliers, job applicants, employees, interns, students, trainees, visitors and other individuals whose personal data ZCHPC processes. It supports compliance with the Cyber and Data Protection Act [Chapter 12:07] (CDPA), applicable regulations and lawful requirements issued by the Data Protection Authority.

### 2. Scope

This policy applies to personal data processed through:

- ZCHPC websites, portals, service desks, email, collaboration platforms and online forms;
- HPC accounts, cloud and hosting services, virtual machines, storage, networking, backup, research platforms and system administration;
- customer onboarding, contracting, billing, support, monitoring and service management;
- research collaborations, training programmes, internships, student placements, events and facility tours;
- employment, recruitment, supplier management and professional engagements; and

- physical security processes, including visitor registers, access-control logs, device authorisations and CCTV where deployed.

### 3. ZCHPC's data-protection roles

#### 3.1 ZCHPC as data controller

ZCHPC acts as a data controller when it determines why and how personal data is processed, for example, for account administration, employment, procurement, billing, facility access, website operations, training, security monitoring and its own regulatory obligations.

#### 3.2 ZCHPC as data processor or service provider

Where a customer, ministry, university, research institution or other organisation places data or workloads on ZCHPC infrastructure and determines the purpose and essential means of processing, that organisation is normally the controller and ZCHPC processes the data on its documented instructions. The applicable service agreement or data processing agreement governs that processing.

Important for hosted data: Questions or rights requests concerning data within a customer-controlled hosted system should normally be directed first to that customer or system owner. ZCHPC will provide reasonable assistance to the controller in accordance with the applicable contract and law.

### 4. Personal data we collect

Depending on the relationship and service, ZCHPC may collect the following categories:

| Category                       | Examples                                                                                                                                                                    |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Identity and contact</b>    | Name, title, identity or passport details where required, photograph, signature, institution, address, telephone number and email.                                          |
| <b>Account and access</b>      | Username, account identifiers, authentication records, access permissions, facility access logs, device details and support history.                                        |
| <b>Customer and commercial</b> | Organisation, contract, quotation, billing, payment, procurement, supplier, project and service-consumption information.                                                    |
| <b>Employment and training</b> | Qualifications, employment history, references, attendance, assessment, internship or placement records, emergency contacts and related HR information.                     |
| <b>Technical and usage</b>     | IP address, browser and device information, operating system, timestamps, job-submission metadata, resource allocation, system logs, network events and diagnostic records. |

|                                           |                                                                                                                                                                                                               |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Security and facility</b>              | Visitor registers, CCTV images where used, incident records, access-card activity, equipment authorisation and physical-security observations.                                                                |
| <b>Communications</b>                     | Enquiries, correspondence, complaints, data-subject requests, meeting records and feedback.                                                                                                                   |
| <b>Sensitive or special-category data</b> | Health, biometric or other sensitive data only where necessary, lawful and subject to enhanced safeguards—for example, access accommodation, emergency response or approved hosted research workloads.        |
| <b>Customer-hosted content</b>            | Personal data contained in datasets, applications, backups or research workloads controlled by a ZCHPC customer. ZCHPC does not routinely inspect this content except as authorised or technically necessary. |

## 5. Sources of personal data

ZCHPC obtains personal data directly from individuals and, where lawful, from:

- their employer, university, research institution, project sponsor or authorised account administrator;
- customers and partners using ZCHPC infrastructure;
- recruitment agencies, referees, suppliers and public authorities;
- systems, networks, access-control devices and security-monitoring tools; and
- publicly available or lawfully accessible sources where verification is necessary.

## 6. Why we process personal data

ZCHPC processes personal data only for specified and legitimate purposes, including to:

- create and administer accounts, allocate computing resources and deliver HPC, cloud, storage, hosting, backup, connectivity and support services;
- authenticate users, manage privileged access, enforce acceptable-use rules and maintain fair resource allocation;
- monitor availability, capacity, performance, cybersecurity and physical security, and investigate incidents or misuse;
- manage customers, projects, contracts, billing, debt collection, procurement, suppliers and professional relationships;
- support research, innovation, collaboration, training, internships, student placements and skills development;
- recruit, employ and manage staff, contractors and secondees;
- respond to enquiries, complaints, data-subject requests, audits and regulatory communications;
- maintain business continuity, disaster recovery, backups and evidential records; and
- meet legal, regulatory, ethical, contractual, reporting and public-interest obligations.

## 7. Legal grounds for processing

Depending on the circumstances and applicable law, ZCHPC relies on one or more lawful grounds, including performance of a contract or steps requested before a contract; compliance with a legal obligation; consent; protection of vital interests; performance of a task in the public interest or exercise of official authority; and legitimate interests that are not overridden by the rights and interests of individuals. Where consent is relied upon, it may be withdrawn without affecting processing already carried out lawfully.

Sensitive personal data is processed only where a lawful additional condition applies and appropriate safeguards are in place. Research teams and customers remain responsible for obtaining ethics approval, consent or other legal authority for datasets they control.

## 8. Research, HPC and customer-hosted workloads

- Customers and researchers must upload only data they are authorised to process and must comply with applicable law, research ethics, contracts and ZCHPC acceptable-use requirements.
- Where practical, personal data should be anonymised, pseudonymised, minimised or encrypted before transfer to ZCHPC systems.
- Project owners must classify data and communicate handling, residency, retention, backup, access and deletion requirements before onboarding high-risk workloads.
- A data protection impact assessment (**DPIA**) should be completed before processing likely to present a high risk, including large-scale sensitive data, systematic monitoring, biometrics, novel technologies or data matching.
- ZCHPC personnel may access customer-hosted data only when authorised and necessary for service delivery, security, recovery, support, legal compliance or incident investigation.
- Customers remain responsible for responding to rights requests and determining lawful retention of customer-controlled content; ZCHPC will assist as contractually required.

## 9. Sharing and disclosure

ZCHPC does not sell or rent personal data. It may disclose data only where necessary and lawful to:

- authorised ZCHPC staff, contractors and governance bodies on a need-to-know basis;
- the individual's employer, institution, project owner or authorised account administrator;
- technology, connectivity, security, professional, payment, maintenance and support providers bound by appropriate confidentiality and data-protection obligations;
- research collaborators or partner institutions under an approved agreement;
- POTRAZ in its capacity as the Data Protection Authority, law-enforcement bodies, courts, auditors or other competent authorities where lawfully required; and
- a successor or authorised party in connection with a lawful restructuring or transfer, subject to appropriate safeguards.

ZCHPC conducts proportionate due diligence and uses contracts or other safeguards when appointing third parties that process personal data on its behalf.

## **10. International and cross-border transfers**

Some support services, collaboration tools, suppliers, researchers or customer configurations may involve access to or storage of personal data outside Zimbabwe. Before a cross-border transfer, ZCHPC will assess the legal basis, destination, risks and required approvals or notifications, and will implement appropriate contractual, organisational and technical safeguards. Customer-controlled cross-border transfers must be authorised in the relevant service documentation.

## **11. Data retention and disposal**

ZCHPC retains personal data only for as long as necessary for the purpose collected, legal and regulatory obligations, contractual requirements, security, research governance, dispute management, audit and business continuity. Retention periods are determined with reference to data category, sensitivity, risk and operational need.

At the end of the applicable retention period, data is securely deleted, anonymised or archived with restricted access. Backup data may remain until it is overwritten through the normal backup cycle. Customer data is returned or deleted in accordance with the service agreement, lawful instructions and any required preservation hold.

## **12. Information security**

ZCHPC applies risk-based technical and organisational safeguards appropriate to the nature of its services and the data involved. Measures may include:

- identity and access management, least privilege, privileged-access controls and periodic access reviews;
- network segmentation, secure configuration, vulnerability and patch management, anti-malware and protective monitoring;
- encryption or other protection for data in transit and at rest where appropriate;
- physical access control, visitor management, environmental controls and CCTV where deployed;
- logging, monitoring, incident response, backup, recovery and business-continuity arrangements;
- confidentiality obligations, awareness training and role-based security responsibilities; and
- supplier due diligence, contractual controls and periodic assurance activities.

No system can be guaranteed completely secure. Individuals and customers must protect credentials, use approved transfer channels, follow security instructions and promptly report suspected compromise.

## **13. Personal data breaches and security incidents**

ZCHPC maintains procedures to identify, contain, assess, investigate, document and remediate suspected personal data breaches. Where required, ZCHPC will notify the Data Protection Authority and affected

individuals within applicable legal timeframes. When ZCHPC acts as a processor, it will notify and assist the relevant controller in accordance with the contract and law.

Suspected loss, unauthorised disclosure, malware, account compromise or misuse involving personal data should be reported immediately to [risk@hpc.ac.zw](mailto:risk@hpc.ac.zw) and [legal@hpc.ac.zw](mailto:legal@hpc.ac.zw), with sufficient information to support prompt containment.

## **14. Your data-protection rights**

Subject to applicable law and lawful limitations, an individual may request:

- confirmation of whether ZCHPC processes their personal data and access to that data;
- correction or completion of inaccurate or incomplete data;
- deletion or erasure where the data is no longer required or processing is unlawful;
- restriction of processing or an objection to particular processing;
- withdrawal of consent where consent is the legal basis;
- information about relevant automated decision-making, where applicable; and
- review of a concern or complaint and escalation to the Data Protection Authority.

Requests should be sent to [risk@hpc.ac.zw](mailto:risk@hpc.ac.zw) and [legal@hpc.ac.zw](mailto:legal@hpc.ac.zw). ZCHPC may verify identity and authority before releasing or changing personal data. If the request concerns a customer-controlled hosted system, ZCHPC may refer the requester to the relevant controller and support that controller as required.

## **15. Cookies and website analytics**

ZCHPC websites may use strictly necessary cookies for security, session management and functionality, and may use optional analytics or preference cookies where permitted. Users can manage cookies through available consent controls and browser settings. Disabling essential cookies may affect website functionality. A service-specific cookie notice should identify the cookies in use, their purpose, provider and duration.

## **16. Children, students, interns and visitors**

ZCHPC may engage students, interns, trainees and visitors through authorised programmes. It will collect only information necessary for participation, supervision, safety, facility access, learning administration and legal obligations. Where a participant is a child, appropriate consent or other lawful authority and enhanced safeguards will be used. Access to data-centre areas, systems and workstations is role-based, supervised and subject to device, confidentiality and cybersecurity requirements.

## **17. Automated decision-making**

ZCHPC does not ordinarily make decisions producing legal or similarly significant effects solely by automated means. If such processing is introduced, ZCHPC will provide appropriate notice, assess the risks and implement safeguards required by law.

## 18. External links and third-party services

ZCHPC websites and services may link to third-party sites or integrate third-party tools. Those organisations may process data under their own privacy notices. ZCHPC is not responsible for independent third-party practices, but it assesses providers where they process personal data on ZCHPC's behalf.

## 19. Accountability, training and policy review

ZCHPC maintains privacy governance arrangements proportionate to its activities, including assigned responsibilities, records of processing, risk assessments, data protection impact assessments, contractual controls, incident records, awareness and periodic compliance review. Staff, contractors, students and authorised users must comply with applicable privacy, confidentiality, acceptable-use and security requirements.

This policy will be reviewed at least annually and when material changes occur in law, technology, services, processing risks or organisational responsibilities. Updated versions will be published through appropriate ZCHPC channels with a revised effective date.

## 20. Complaints and contact details

| Contact                          | Details                                                                            |
|----------------------------------|------------------------------------------------------------------------------------|
| ZCHPC Data Protection Department | <a href="mailto:risk@hpc.ac.zw/legal@hpc.ac.zw">risk@hpc.ac.zw/legal@hpc.ac.zw</a> |
| Postal / physical address        | Zimbabwe Science Park 1, 630 Churchill Avenue, Mount Pleasant, Harare, Zimbabwe    |
| Telephone                        | +263 712 563 563 / +263 772 779 730                                                |
| Website                          | <a href="https://hpc.ac.zw">https://hpc.ac.zw</a>                                  |

ZCHPC will investigate privacy concerns fairly and promptly. An individual may also lodge a complaint with POTRAZ in its role as Zimbabwe's Data Protection Authority. This does not affect any other lawful remedy.

**Executive Sponsor: Director, ZCHPC**

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

**Authorized Approver: Chairperson, ZCHPC Committee**

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

