POPIA Compliance Document for CS Department

1. Purpose and Scope

This document outlines how the Computer Science (CS) Department at the University of Pretoria complies with the Protection of Personal Information Act (POPIA) in relation to the collection, storage, transfer, and sharing of personal information. It covers all systems and processes that handle personal data, including the CS Portal, LDAP directory, attendance features, tutor appointment documentation, and external interactions (e.g., plagiarism detection). Only applications specific to the CS Department are elaborated on. For a broader view of UP privacy policies please visit the official UP website. For any queries regarding this document or regarding how personal information is used, please contact popia@cs.up.ac.za.

2. Definitions

- **Personal Information**: Any information relating to an identifiable living individual, including names, student numbers, IP addresses, location data, and documentation uploaded for tutor appointments.

- **Processing**: Any operation or activity concerning personal information, such as collection, receipt, recording, organization, storage, updating, retrieval, dissemination, or deletion.

- **Operator**: External entity processing personal information on behalf of the CS Department (e.g., MOSS plagiarism detector).

- **Transfer**: Transmission of personal information to a third party or recipient, including entities outside the department or foreign countries.

- **TechTeam:** Staff members serving as technical assistants within the department. TechTeam members are granted administrative access to CS Department services and are responsible for maintaining the integrity, security, and privacy of user information stored within these systems.

3. Lawful Basis for Processing

All personal information processed by the CS Department is necessary for:

1. **Administration**: Managing user accounts, course enrollments, and departmental records.

2. **Authentication**: Verifying user identities when accessing the CS Portal and related services (usernames linked to personal information).

3. **Academic Functions**: Attendance tracking, tutor appointments, and plagiarism detection.

Section 4 expands on the lawful bases in greater detail.

4. Personal Information Collected

Data Category	Source	Purpose
Usernames, passwords, names	CS Portal user creation	Authentication, admin
Student lists (names, student numbers)	Institutional records upload	LDAP population, enrollment
Tutor appointment documents	Student uploads via CS Portal	Academic support
IP address, location	Attendance feature	Attendance verification

4.1 Usernames, passwords, names and student lists.

All CS Department services that require authentication make use of user accounts linked to each student, staff member, or affiliated person. For administrative purposes and CS-related communication, it is necessary to store personal identifiers such as names, email addresses, and student numbers to manage access, maintain accurate records, and ensure effective departmental correspondence.

Data flows:

1. **Collection**
    - Student lists and module registrations from DESA (Department of Enrolment and Student Administration) are transferred to a CS server once a day.
    - Staff details are recorded when a staff account is created on the CS Portal by a member of TechTeam.
    - User passwords are collected and managed through the CS Portal's user-management interface.

2. **Authentication**
   Users are authenticated for CS services via their CS usernames and passwords. The list of services includes but is not limited to:
    - portal.cs.up.ac.za
    - ff.cs.up.ac.za
    - wheatley.cs.up.ac.za
    - jupyterhub.cs.up.ac.za
    - hyperperform.cs.up.ac.za
    - overleaf.cs.up.ac.za

- owncloud.cs.up.ac.za
- Informatorium Lab[1] Linux Image[2] authentication

3. **Provisioning & Role Assignment**
   Users receive a predefined role which defines their privileges and governs access to protected resources.

4. **Student-List Distribution**
   Authenticated users (administrators and course staff) can view student list details—names, student numbers, and emails—through the access-controlled CS Portal.

5. **Storage & Backup**
   CS Portal user details/personal identifiers are stored in a database on a secured server. Data is backed up to a NAS (Network Attached Storage).

6. **Access Control**
   Authentication and an appropriate user role are required to view or modify user information. Access to personal identifiers—such as names, student numbers, and email addresses—is strictly controlled and limited to authorized personnel only.

7. **Deletion & Retention**
   Student user accounts are archived after one year of inactivity. When a staff member leaves the department, a TechTeam member manually archives their account. These practices help ensure that personal data is not retained longer than necessary.

Lawful basis:
In accordance with the Protection of Personal Information Act (POPIA), personal identifiers such as names, email addresses, and student numbers are collected and processed to manage access to Computer Science Department services that require authentication. This processing is necessary for administrative purposes, maintaining accurate records, and ensuring effective communication with students, staff, and affiliated individuals in support of the Department's operational responsibilities.

4.2 Tutor appointment documents

Tutor appointment documents are retained to streamline the administrative process required for appointing student tutors. These documents are necessary for the department to fulfil its contractual and legal obligations related to student employment.

Data flows:

1. **Collection**

[1] The Informatorium consists of 12 Computer labs furnished with high-end, latest generations computers.
[2] Linux operating system customized for the needs of CS students

Tutor applicants submit their documents on the CS Portal upon applying for the position.

2. **Review and Approval**
   Course coordinators review the submitted documents in order to shortlist candidates for the position.

3. **Document retention**
   Tutor appointment documents are retained only for the duration of the semester in which the tutor is employed, for purposes related to Human Resources (HR). All such documents are deleted at the end of each semester.

Lawful basis:
In accordance with the Protection of Personal Information Act (POPIA), tutor appointment documents are retained to support the efficient administration of student tutor appointments. The processing of this information is necessary for the Department to fulfil its contractual obligations to student employees, as well as to comply with legal and regulatory requirements related to employment and Human Resources administration.

4.3 IP address and location

To capture valid attendance records, IP addresses are logged to verify that students are connected to the UP network, and location data is collected to ensure that the student marking attendance is physically near the venue where the lecture or tutorial took place.

Lawful basis:
In accordance with the Protection of Personal Information Act (POPIA), personal information such as IP addresses and location data is collected and processed on the basis of the Department's legitimate interest in ensuring the integrity of attendance records. This processing is necessary to confirm that students marking attendance are physically present at the venue and connected to the University of Pretoria's network at the time of the lecture or tutorial. The information is used solely for this purpose and is handled with appropriate safeguards to protect student privacy.

5. Storage and Retention

- **LDAP Directory**: All user and student information is stored in the department's LDAP service, which is access-controlled.

- **CS Portal Database**: Data at rest is stored on secure servers.

- **Retention Period**: Personal information is retained only for as long as necessary to fulfill academic and administrative purposes, after which it is securely deleted. In general, personal information is kept for one year, although backup data may persist for five years or longer to support recovery and continuity needs.

6. Transfer and Sharing

- **Internal Sharing**: Displaying staff profiles on the CS website constitutes internal sharing.

- **External Transfer**: The only external transfer is sending code files to the MOSS plagiarism detection service; no personal datasets are transferred.

- **International Transfer**: There are currently no known transfers of personal information to foreign recipients. Should such transfers become necessary in the future, this compliance document will be amended accordingly.

7. Security Measures

- **Access Control**:
    - CS Portal; only authorized staff can view or modify personal data.
    - The LDAP directory is only accessible via a local wired network with controlled access points.

- **Encryption**: All websites that serve personal information are accessed via HTTPS and follow industry-standard security best practices for data in transit.

- **Breach Notification Measures:** In the event of a data breach involving personal information, TechTeam must be notified immediately. TechTeam will investigate the incident and notify any affected users accordingly.

8. Data Subject Rights

Individuals have the right to:

1. **Access** their personal information held by the department.

2. **Rectify** inaccurate or incomplete data.

3. **Object** to processing in certain circumstances.

4. **Request deletion** of data when no longer necessary.

Requests can be submitted to the departmental POPIA Officer at popia@cs.up.ac.za / linda.marshall@up.ac.za / asingh@cs.up.ac.za.

9. Procedure for Handling POPIA Compliance Queries

A procedure is established to ensure that all queries related to the Protection of Personal Information Act (POPIA) are addressed promptly, transparently, and in accordance with legal and institutional requirements.

1. **Designated Contact Point**
   The designated contact point for POPIA Compliance Queries is the popia@cs.up.ac.za email address.

2. **Initial assessment**
   Determine whether the query relates to:

   - Data access or correction (Data Subject Request)
   - Data collection, use, or retention
   - Data breach concerns
   - General information about POPIA compliance

   Categorize the query and assign priority based on potential risk or urgency.

3. **Escalation and Response**
   If the query is complex or may expose legal risk, escalate to the University's Legal Services or the Institutional Information Officer.
   Provide a substantive response within 10 working days, or notify the requester of any delays with an expected timeframe.

4. **Review and Feedback**
   If the query indicates a gap in current practices or policies, refer the issue to the departmental POPIA task group (TechTeam) or relevant administrative structure for review. Implement corrective actions where necessary.

10. Responsibilities

- **POPIA Officer**: Oversees compliance, handles data subject requests, and conducts periodic audits.

- **System Administrators**: Ensure secure configuration of LDAP, databases, and servers.

- **Academic Staff**: Handle personal information in accordance with this policy.

11. Review and Updates

This document will be reviewed annually or upon significant changes to systems or processes.