Privacy Policy and Terms of Use

1 Introduction

Welcome to the **Online Test Monitoring System**. This document outlines our policies regarding the collection, use, and protection of user data, as well as the terms governing the use of our platform. By using this system, you agree to comply with the policies stated herein.

2 Data Collection and Usage

We collect and process personal data to facilitate online test monitoring and fraud detection. This may include:

- **User-provided information:** Candidate and sponsor email addresses.
- **Webcam feed:** Captured in real-time for monitoring purposes.
- **Detection results:** AI-generated analysis of face authenticity.

2.1 Purpose of Data Collection

The collected data is used exclusively for:

- Identifying and verifying users during online tests.
- Detecting potential fraud or spoofing attempts.
- Generating session reports for exam administrators.

2.2 Data Retention

We do not store personal data beyond the necessary duration for exam monitoring. Once the session ends, data is processed and may be temporarily stored for fraud analysis before automatic deletion.

3 User Responsibilities

By using this system, users agree to:

- Provide accurate and truthful information.
- Allow temporary access to their webcam for monitoring purposes.
- Refrain from attempting to bypass or manipulate the AI detection system.

Misuse of the platform, including fraudulent activity or unauthorized access, may result in termination of service and reporting to relevant authorities.

4 AI System Limitations

The **Online Test Monitoring System** uses artificial intelligence for fraud detection. As a probabilistic tool, AI does not guarantee 100% accuracy. Users acknowledge that:

- The system may generate false positives or false negatives.
- Decisions should not be made solely based on AI analysis without human review.
- The developers are not responsible for errors or misclassifications made by the AI model.

5 Data Protection and Security

We implement security measures to protect user data from unauthorized access, alteration, or misuse. However, users should understand that no digital system is completely secure. Key protections include:

- **End-to-end encryption** of sensitive data transmissions.
- **Restricted access** to stored data, accessible only to authorized personnel.
- **Automatic data deletion** after a predefined retention period.

Despite these safeguards, users should exercise caution when sharing personal information online.

6 Third-Party Services

Our system may integrate third-party services (e.g., email services for notifications). These services operate under their own privacy policies, and we are not responsible for their data handling practices.

7 Changes to This Policy

We reserve the right to update this Privacy Policy and Terms of Use at any time. Any changes will be communicated through the platform, and continued use of the system implies acceptance of the revised terms.

8 Contact Information

For inquiries regarding this policy or data protection concerns, please contact us at:

- **knazarenko@mun.ca**
- **glemoullec@mun.ca**
- **mohsen@mun.ca**
- **fmoquet@mun.ca**

By using this system, you acknowledge that you have read, understood, and agree to this Privacy Policy and Terms of Use.