SOP Template: Verification of Complainant's Identity and Authorization

This SOP details the process for **verification of complainant's identity and authorization**, ensuring that complainants are accurately identified and properly authorized before proceeding with any complaint handling. It covers steps for verifying personal information, validating authorization documents, safeguarding confidential information, and maintaining compliance with legal and organizational requirements to protect both the complainant and the organization.

1. Purpose

To establish a standardized process for verifying the identity and authorization of individuals submitting complaints to ensure the integrity and legal compliance of the complaint management process.

2. Scope

This SOP applies to all staff members involved in receiving and processing complaints from individuals, representatives, or third-party entities.

3. Responsibilities

- **Complaint Handler:** Carries out the verification process and maintains records.
- **Supervisor:** Reviews verifications for compliance with procedures.
- **Data Protection Officer:** Ensures safeguarding of personal and confidential information.

4. Definitions

- **Complainant:** An individual or agent submitting a complaint to the organization.
- **Authorization:** Document or proof granting a representative authority to act on behalf of a complainant.
- **Personal Information:** Any data used to uniquely identify an individual.

5. Procedure

1. **Receipt of Complaint**
    - Log incoming complaints with preliminary details.
    - Inform complainant of the need for identity and authorization verification.
2. **Verification of Complainant's Identity**
    - Request government-issued photo ID (e.g., passport, driver's license).
    - Cross-check provided information against records, if available.
    - Ensure information is current and matches the complainant's details.
3. **Validation of Authorization (if applicable)**
    - Request a signed and dated authorization letter or legal document.
    - Verify document authenticity, including signatures and contact information of the principal.
    - If necessary, contact the principal to confirm authorization.
4. **Safeguarding Confidential Information**
    - Store copies of identification and authorization securely and restrict access.
    - Ensure compliance with data protection regulations and internal policies.
5. **Record Keeping**
    - Document the verification process, including date, name, and staff involved.
    - Retain records in accordance with retention schedules and privacy laws.
6. **Compliance Check**
    - Supervisor reviews that steps were completed and authorizes advancement of complaint handling.

6. Documentation

Maintain the following records:

- Copy of complainant's identification
- Authorization documentation
- Verification checklist
- Complaint intake form
- Supervisor verification record

7. Compliance and Confidentiality

- Adhere to all applicable data protection, privacy, and organizational policies.
- Only authorized personnel may access verification data.
- Destroy verification data securely once no longer required under law or policy.

8. References

- Applicable data protection laws (e.g., GDPR, HIPAA)
- Organization's Privacy Policy
- Record Retention Policy

9. Revision History

Date	Version	Description	Author
2024-06-01	1.0	Initial SOP Release	[Your Name/Dept]