DOCUMENT RETENTION AND MANAGEMENT POLICY

TABLE OF CONTENTS

POLICY REVIEW HISTORY

Review Date	Reviewed By	Changes/Updates Made	Reason for Changes	Next Review Date
January 10, 2022	Executive Director	Initial policy creation and implementation	Establishment of document retention framework for PY	January 2023
January 15, 2023	Records Manager	Updated retention periods and added digital security protocols	Compliance with new regulatory requirements and donor policies	January 2024
August 25, 2023	Policy Review Team	Enhanced document destruction and physical record security	Strengthening data protection and operational security	August 2024
December 10, 2024	Executive Director	Added advanced encryption for digital records and improved access control for physical documents	Adapting to evolving cybersecurity threats and ensuring compliance with new international data protection laws	January 2026

Approval Statement

Policy Title: Document Retention and Management Policy
Policy Code: PY30003004
Approval Date: December 10, 2024

Statement of Approval:
The Board of Directors of Peace by Youth (PY) formally approves the adoption and implementation of the Document Retention and Management Policy. This policy has been reviewed and endorsed as a crucial framework for ensuring the systematic retention, secure management, and timely disposal of documents and records in compliance with legal, regulatory, and operational requirements.

The Document Retention and Management Policy establishes clear guidelines for classifying, storing, accessing, and preserving PY's critical records while ensuring that non-essential records are securely disposed of. It reflects PY's commitment to transparency, accountability, and operational excellence, aligning with its mission to empower youth, foster peace, and advance socio-economic development.

Implementation and Review:
This policy will be disseminated to all relevant stakeholders and rigorously implemented across PY's operations. It will be subject to regular review and updates to ensure alignment with best practices, organizational priorities, and emerging regulatory requirements.

Signatures:

Chairperson, Board of Directors
Name: Nisar Ahmed

Signature: ____________________
Date: December 10, 2024.

Secretary, Board of Directors
Name: Hina Jamil

Signature: ____________________
Date: December 10, 2024.

1. PURPOSE

The purpose of this policy is to establish comprehensive guidelines for the retention, management, and disposal of documents and records maintained by Peace by Youth (PY) in accordance with legal, regulatory, and operational requirements. It is essential for Peace by Youth (PY) to have a structured and effective document retention policy to ensure that crucial documents are available when needed for regulatory, audit, historical, and operational purposes, while also ensuring that non-essential records are disposed of securely and timely.

By adopting this policy, Peace by Youth (PY) aims to:

- Ensure compliance with all applicable legal and regulatory requirements regarding document retention.
- Provide a systematic approach to managing the lifecycle of documents from creation, retention, storage, to their eventual destruction or archival.
- Protect sensitive and confidential information from unauthorized access or disclosure.
- Reduce the risk of legal or financial penalties by ensuring the availability of documents necessary for audits, legal disputes, or regulatory inquiries.
- Minimize the cost and space involved in storing unnecessary records.
- Preserve documents of historical or strategic importance to Peace by Youth (PY).

The retention of records and documents should be done with careful attention to the long-term and short-term needs of the organization, ensuring that the right information is kept and accessible, while outdated or unnecessary information is securely disposed of to free up storage and improve data management practices.

2. SCOPE

This policy applies to all employees, board members, volunteers, contractors, consultants, and other representatives of Peace by Youth (PY) involved in creating, receiving, maintaining, storing, or disposing of documents and records. It covers all types of records regardless of their format, including physical (paper-based) and digital records. The policy is designed to be comprehensive and applies to documents stored in physical archives, digital servers, cloud storage, emails, and external media such as USB drives or DVDs.

The scope includes, but is not limited to:

- **Governance records**: Board meeting minutes, organizational bylaws, and regulatory filings.
- **Financial records**: Invoices, audited financial statements, tax documents, and financial policies.
- **Human resource records**: Employee contracts, performance reviews, and human resource policies.
- **Programmatic records**: Documents related to program planning, monitoring, evaluation, and reporting.
- **Legal records**: Contracts, Memoranda of Understanding (MoUs), legal correspondence, and court documents.
- **Operational records**: Procurement documents, partnership agreements, and internal reports.
- **Communications**: Emails, memos, marketing materials, and meeting notes.

All stakeholders of Peace by Youth (PY) are responsible for ensuring that documents within their control are maintained and disposed of according to the guidelines laid out in this policy. In cases where specific regulatory or contractual obligations apply, the more stringent retention requirement should take precedence.

3. DOCUMENT CATEGORIES AND RETENTION PERIODS

This section provides detailed guidelines on the retention periods for specific types of documents. The retention periods have been determined based on their importance for legal compliance, operational needs, financial audits, donor reporting, and organizational history. Each document category is assigned a unique reference code and a rationale for its retention period, ensuring that documents are kept for the appropriate duration.

3.1 GOVERNANCE DOCUMENTS (1000 SERIES)

Governance documents are fundamental to Peace by Youth's (PY) legal structure and operational oversight. They are essential for ensuring that the organization complies with applicable laws and regulations, and they provide a historical record of key decisions made by the Board of Directors and other governing bodies.

1. **Memorandum of Association (MoA)**
    - **Reference Code**: PY0010001001
    - **Retention Period**: **Permanent**
    - **Rationale**: The Memorandum of Association (MoA) is a critical legal document that outlines the purpose, authority, and limitations of Peace by Youth (PY). It is the organization's charter and must be retained indefinitely as it forms the legal basis for its operations and interactions with stakeholders, including donors, regulatory authorities, and beneficiaries. The MoA is often required for legal audits, government filings, and compliance purposes.
2. **Articles of Association (AoA)**
    - **Reference Code**: PY0010001002
    - **Retention Period**: **Permanent**
    - **Rationale**: The Articles of Association (AoA) govern the internal operations of Peace by Youth (PY), specifying the roles and responsibilities of board members, voting procedures, and decision-making processes. These articles are crucial for maintaining transparency in the governance structure and ensuring the integrity of organizational processes. As a key governance document, it must be retained permanently to provide ongoing guidance on organizational practices.
3. **Registration Certificate**
    - **Reference Code**: PY0010001003
    - **Retention Period**: **Permanent**
    - **Rationale**: The Registration Certificate is a legal document issued by the relevant authorities that formally acknowledges the incorporation and legal status of Peace by Youth (PY). This certificate is critical for proving the organization's legal status, applying for grants, entering into contracts, and ensuring compliance with local laws. It must be kept permanently to demonstrate that the organization is legally recognized and authorized to operate.
4. **Board of Directors (BoD) List and Profiles**
    - **Reference Code**: PY0010001004
    - **Retention Period**: **10 years after service ends**
    - **Rationale**: The list of Board of Directors and their profiles contain key information about the individuals responsible for the governance of Peace by Youth (PY). These records are essential for ensuring transparency in leadership, allowing for reference during legal disputes or audits, and for maintaining an accurate governance history. Retaining these records for 10 years after a director's service ends allows the organization to maintain accountability and reference leadership decisions made during their tenure.
5. **Organizational Bylaws**
    - **Reference Code**: PY0010001005
    - **Retention Period**: **Permanent**

    - **Rationale**: Organizational bylaws outline the rules and procedures for the governance of Peace by Youth (PY), including the roles and responsibilities of board members, voting procedures, and meeting protocols. These bylaws provide the framework for the organization's internal governance and must be retained permanently to ensure consistency in governance practices and compliance with legal standards. They are often required for legal audits and regulatory reviews.
6. **Minutes of Board Meetings**
    - **Reference Code**: PY0010001006
    - **Retention Period**: **7 years**
    - **Rationale**: Minutes of board meetings serve as the official record of decisions made by the Board of Directors and other governing bodies. These records are essential for demonstrating compliance with governance procedures, documenting strategic decisions, and providing transparency to stakeholders. Retaining board meeting minutes for seven years ensures that the organization can reference these decisions for auditing purposes, legal disputes, and organizational history.

3.2 FINANCIAL DOCUMENTS (2000 SERIES)

Financial documents are essential for demonstrating Peace by Youth's (PY) financial accountability, transparency, and compliance with regulatory and donor requirements. Retaining these documents ensures that financial transactions are properly recorded, audited, and reported to stakeholders.

1. **Annual Financial Statements (Audited)**
    - **Reference Code**: PY0010002001
    - **Retention Period**: **10 years**
    - **Rationale**: Annual financial statements provide a comprehensive summary of Peace by Youth's (PY) financial performance, including income, expenses, assets, and liabilities. These statements are essential for demonstrating financial transparency to donors, regulatory authorities, and auditors. Retaining audited financial statements for 10 years ensures compliance with tax and audit regulations and provides a long-term financial history of the organization.
2. **Income and Expenditure Records**
    - **Reference Code**: PY0010002002
    - **Retention Period**: **7 years**
    - **Rationale**: Income and expenditure records detail all financial transactions conducted by Peace by Youth (PY), including donations, grants, payments, and operational expenses. These records are required for financial audits, tax filings, and donor reporting. Retaining these records for seven years ensures compliance with local tax laws and audit requirements, while providing sufficient historical data for financial management.
3. **Finance and Accounting Policy**
    - **Reference Code**: PY0010002003
    - **Retention Period**: **Permanent**
    - **Rationale**: The finance and accounting policy governs the financial management procedures of Peace by Youth (PY), ensuring that all transactions are recorded and managed according to established standards. This policy must be retained permanently to provide ongoing guidance on financial practices, ensure compliance with regulatory requirements, and maintain transparency in financial management.
4. **Procurement Policy**
    - **Reference Code**: PY0010002004
    - **Retention Period**: **Permanent**
    - **Rationale**: The procurement policy outlines the procedures for purchasing goods and services for Peace by Youth (PY). It ensures that procurement processes are conducted transparently and fairly, in compliance with donor requirements

and organizational standards. Retaining this policy permanently provides a reference for ensuring accountability in procurement activities and minimizing the risk of fraud or mismanagement.

5. **Tax Exemption Certificates (if applicable)**
   - **Reference Code**: PY0010002005
   - **Retention Period**: **Permanent**
   - **Rationale**: Tax exemption certificates provide proof of Peace by Youth's (PY) status as a tax-exempt organization. These certificates are essential for demonstrating compliance with tax laws and ensuring that the organization benefits from tax exemptions. Retaining them permanently ensures that the organization can provide proof of its tax status whenever needed.

3.3 OPERATIONAL DOCUMENTS (3000 SERIES)

Operational documents are critical for documenting the day-to-day activities and partnerships of Peace by Youth (PY). These documents ensure that the organization remains compliant with internal policies and external regulatory obligations while providing a record of programmatic initiatives and partnerships.

1. **Annual Progress Reports**
   - **Reference Code**: PY0010003001
   - **Retention Period**: **10 years**
   - **Rationale**: Annual progress reports document the key achievements, challenges, and outcomes of Peace by Youth's (PY) programs and initiatives. These reports are used for internal evaluation, donor reporting, and stakeholder communication. Retaining these reports for 10 years ensures that the organization has a comprehensive history of its programmatic activities and can provide evidence of impact to donors and regulatory bodies.
2. **Partnership Agreements or MoUs**
   - **Reference Code**: PY0010003002
   - **Retention Period**: **7 years after expiration**
   - **Rationale**: Partnership agreements and Memoranda of Understanding (MoUs) outline the terms and conditions of Peace by Youth's (PY) collaborations with external organizations. These documents are legally binding and must be retained for seven years after their expiration to ensure that the organization can reference the terms of these agreements if any legal or operational issues arise.
3. **Cash and Voucher Assistance (CVA) Policy**
   - **Reference Code**: PY0010003003
   - **Retention Period**: **Permanent**
   - **Rationale**: The Cash and Voucher Assistance (CVA) policy governs the distribution of financial aid in the form of cash or vouchers to beneficiaries. This policy is critical for ensuring transparency and accountability in the disbursement of funds. It must be retained permanently to provide ongoing guidance for programmatic activities involving cash or voucher distributions.

3.4 HUMAN RESOURCE DOCUMENTS (4000 SERIES)

Human resource documents are essential for managing the personnel records of Peace by Youth (PY), ensuring compliance with labor laws, and maintaining a professional and fair working environment.

1. **Human Resource (HR) Policy**
   - **Reference Code**: PY0010004001
   - **Retention Period**: **Permanent**
   - **Rationale**: The human resource policy governs the recruitment, management, and termination of employees and volunteers. It provides guidelines for maintaining a fair and transparent working environment, in compliance with local labor laws. This policy must be retained permanently to ensure consistency in HR practices and legal compliance.
2. **Code of Conduct and Ethics**

    - **Reference Code**: PY0010004002
    - **Retention Period**: **Permanent**
    - **Rationale**: The code of conduct outlines the ethical standards expected of employees, board members, and volunteers at Peace by Youth (PY). It is essential for maintaining the integrity of the organization and preventing conflicts of interest or unethical behavior. This document must be retained permanently to ensure that all stakeholders adhere to the organization's values and principles.
3. **Grievance Redressal Policy**
    - **Reference Code**: PY0010004003
    - **Retention Period**: **Permanent**
    - **Rationale**: The grievance redressal policy provides a framework for addressing employee complaints and resolving disputes in a fair and transparent manner. This policy must be retained permanently to ensure compliance with labor laws and maintain a fair working environment for all staff.
4. **Whistleblower Policy**
    - **Reference Code**: PY0010004004
    - **Retention Period**: **Permanent**
    - **Rationale**: The whistleblower policy ensures that employees, volunteers, and board members can report misconduct, fraud, or other unethical behavior without fear of retaliation. It is a key component of Peace by Youth's (PY) commitment to transparency and accountability. This policy must be retained permanently to ensure that individuals are protected when reporting misconduct.
5. **Conflict of Interest Policy**
    - **Reference Code**: PY0010004005
    - **Retention Period**: **Permanent**
    - **Rationale**: The conflict of interest policy ensures that employees, volunteers, and board members disclose any personal or financial interests that could influence their decision-making or actions. This policy is essential for maintaining transparency and preventing unethical behavior. It must be retained permanently to ensure that conflicts of interest are identified and managed appropriately.

3.5 PROGRAMMATIC DOCUMENTS (5000 SERIES)

Programmatic documents detail the planning, execution, and evaluation of Peace by Youth's (PY) initiatives. These documents are essential for ensuring compliance with donor requirements and maintaining transparency in program implementation.

1. **Child Protection Policy (if applicable)**
    - **Reference Code**: PY0010005001
    - **Retention Period**: **Permanent**
    - **Rationale**: The child protection policy outlines the procedures and safeguards in place to protect children from harm in all Peace by Youth (PY) programs and activities. This policy must be retained permanently to ensure compliance with child protection laws and donor requirements.
2. **Gender and Inclusion Policy**
    - **Reference Code**: PY0010005002
    - **Retention Period**: **Permanent**
    - **Rationale**: The gender and inclusion policy promotes gender equality and the inclusion of marginalized groups in Peace by Youth's (PY) programs and activities. This policy must be retained permanently to ensure that the organization continues to promote diversity, equity, and inclusion.
3. **Anti-Fraud and Corruption Policy**
    - **Reference Code**: PY0010005003
    - **Retention Period**: **Permanent**

    - **Rationale**: The anti-fraud and corruption policy ensures that Peace by Youth (PY) operates with integrity and accountability, preventing fraudulent activities and corruption in its operations. This policy must be retained permanently to safeguard the organization's ethical standards and reputation.
4. **Inclusive Safeguarding Framework for Persons with Disabilities**
    - **Reference Code**: PY0010005004
    - **Retention Period**: **Permanent**
    - **Rationale**: The inclusive safeguarding framework ensures that persons with disabilities are protected and included in all Peace by Youth (PY) programs and activities. This policy must be retained permanently to ensure compliance with disability rights laws and donor requirements.
5. **MEAL (Monitoring, Evaluation, Accountability, and Learning) & IM Standards and Guidelines**
    - **Reference Code**: PY0010005005
    - **Retention Period**: **7 years**
    - **Rationale**: The MEAL standards and guidelines provide the framework for monitoring and evaluating Peace by Youth's (PY) programs, ensuring that the organization meets its accountability and learning objectives. These documents must be retained for seven years to ensure compliance with donor reporting requirements and to facilitate program improvement.
6. **Modern Slavery Policy**
    - **Reference Code**: PY0010005006
    - **Retention Period**: **Permanent**
    - **Rationale**: The modern slavery policy ensures that Peace by Youth (PY) complies with laws prohibiting forced labor and human trafficking. This policy must be retained permanently to demonstrate the organization's commitment to ethical labor practices.
7. **Humanitarian Policy**
    - **Reference Code**: PY0010005007
    - **Retention Period**: **Permanent**
    - **Rationale**: The humanitarian policy governs Peace by Youth's (PY) response to emergencies and humanitarian crises. This policy must be retained permanently to ensure compliance with international humanitarian standards and donor requirements.

4. DOCUMENT STORAGE AND SECURITY

The safe storage and security of documents are critical to the integrity, confidentiality, and efficiency of Peace by Youth (PY). Whether records are stored digitally or physically, stringent security measures must be implemented to prevent unauthorized access, data breaches, and physical damage.

Effective document storage practices help mitigate risks related to data theft, loss, or damage, ensuring that records remain accessible for legal, regulatory, operational, and historical purposes. The following guidelines define how both digital and physical records must be managed.

4.1 DIGITAL RECORDS

Digital records are particularly susceptible to cyber threats, including hacking, data breaches, and accidental deletion. As such, special care must be taken to ensure the confidentiality, integrity, and availability of electronic documents. Peace by Youth (PY) will implement industry best practices for data security to protect sensitive and confidential information.

4.1.1 Secure Servers

All digital records must be stored on secure servers with encryption protocols that meet or exceed industry standards. These servers must be housed in secure data centers that have controlled access and robust physical security. Any third-party cloud service providers utilized by Peace by Youth (PY) for digital record storage must be certified and compliant with international data protection standards, such as GDPR (General Data Protection Regulation) or ISO 27001 (Information Security Management).

4.1.2 Encryption

Digital records containing sensitive or confidential information must be encrypted both at rest (when stored) and in transit (when being transmitted across networks). Encryption ensures that even if unauthorized individuals gain access to the data, they cannot read or manipulate it without the appropriate decryption keys. All encryption methods used should meet current industry standards for secure encryption algorithms.

4.1.3 Access Controls

Only authorized personnel shall have access to sensitive digital records. Access rights must be managed using a robust authentication system that requires unique user IDs and strong passwords. Wherever possible, multi-factor authentication (MFA) should be implemented to add an extra layer of security for accessing critical systems and documents.

4.1.4 Regular Backups

To safeguard against data loss due to hardware failure, accidental deletion, or cyber-attacks, regular backups of all digital records must be conducted. Backups should be stored in geographically separate locations from the primary data center to ensure business continuity in the event of a disaster. Backup frequency should align with the criticality of the data, with daily or weekly backups for operational documents and more frequent backups for high-priority or sensitive information.

4.1.5 Data Integrity and Monitoring

Monitoring systems must be in place to detect unauthorized access or tampering with digital records. Regular audits and system checks must be conducted to ensure the integrity of stored data. Any unauthorized access attempts or data breaches should be reported immediately to the system administrator and documented according to the incident response protocol.

4.1.6 Secure File Transfers

When sharing digital records externally, secure file transfer protocols (e.g., SFTP, FTPS) must be used to prevent unauthorized interception. Emailing sensitive information should be avoided, and if necessary, documents should be encrypted before sending, and passwords should be shared through separate communication channels.

4.2 PHYSICAL RECORDS

Although digital records are the standard for most modern organizations, certain documents may still be retained in physical form, either due to legal requirements or specific operational needs. Physical records must be handled with the same level of care as digital records to prevent unauthorized access, damage, or loss.

4.2.1 Secure Storage Facilities

All physical records should be stored in secure areas of Peace by Youth's (PY) offices or designated storage facilities. Access to these facilities must be restricted to authorized personnel only, and security measures such as keycard access, visitor logs, and surveillance systems should be implemented to monitor and control entry.

4.2.2 Locked, Fireproof Cabinets

Sensitive or confidential physical records, such as financial documents, personnel files, or legal agreements, must be stored in locked cabinets that are both fireproof and waterproof. These cabinets will protect documents from physical threats such as fire, flooding, or unauthorized access. Only designated personnel should have access to the keys or security codes for these cabinets.

4.2.3 Environmental Controls

Physical records must be stored in an environment that protects them from deterioration due to moisture, heat, or pests. Storage areas must have temperature and humidity controls, and records should be stored in acid-free folders or boxes to prevent yellowing or degradation over time.

4.2.4 Controlled Access

Access to physical records must be tightly controlled. Only authorized personnel should be able to retrieve, view, or handle physical records. Each department is responsible for maintaining an access log that documents when records are removed from storage and by whom. Records should be returned to their secure location as soon as they are no longer needed for active use.

4.2.5 Document Tracking

For physical records, a tracking system should be implemented to ensure that each document can be accounted for at all times. This system may include barcodes, reference numbers, or a manual tracking sheet that records the location and status of each document. The tracking system will prevent documents from being misplaced or lost during transitions between departments or external storage locations.

4.2.6 Archival Storage

Certain physical records, such as historical documents or legal agreements, may need to be archived for long-term retention. Archival storage facilities must meet stringent security and environmental standards to ensure that these records remain intact and accessible for the duration of their retention period.

5. DOCUMENT DESTRUCTION AND DISPOSAL

When documents have reached the end of their designated retention period, it is essential to dispose of them securely and in a manner that protects the confidentiality of sensitive information. Improper disposal of records can expose Peace by Youth (PY) to significant risks, including legal penalties, data breaches, and reputational damage.
The method of document destruction will vary depending on whether the record is stored digitally or physically, but all disposal practices must prioritize security and confidentiality.

5.1 DIGITAL RECORDS

Digital records that are no longer required must be permanently deleted from all servers, cloud storage systems, and devices. Simply moving a file to the "Recycle Bin" or "Trash" is not sufficient for secure disposal. The following procedures outline the correct steps for securely destroying digital records.

5.1.1 Secure Deletion

When digital records are deleted, they must be removed in such a way that the data cannot be recovered by unauthorized individuals. This can be achieved through secure deletion methods, such as data wiping or the use of software specifically designed to overwrite the data multiple times. Peace by Youth (PY) will implement secure deletion tools that meet industry standards, ensuring that all traces of the file are eliminated.

5.1.2 Cloud Storage Deletion

For records stored on third-party cloud storage platforms, it is critical to ensure that deleted files are permanently erased from all servers and backups maintained by the cloud provider. Peace by Youth (PY) will work with its cloud service providers to confirm that once files are marked for deletion, they are irreversibly removed from all systems, including redundant backup locations.

5.1.3 Device Disposal

When electronic devices such as computers, hard drives, or USB drives that store digital records are no longer in use, they must be securely disposed of or recycled. Prior to disposal, all data must be securely wiped from the device using specialized software or by physically destroying the storage media (e.g., shredding the hard drive). The destruction of devices must be documented, and certificates of destruction obtained from third-party service providers where applicable.

5.1.4 Digital Disposal Records

Each instance of digital document destruction must be logged in a **Digital Disposal Record**. This record should include the document name, its reference code, the category under which it falls, the date of destruction, and the method of deletion. This ensures that there is a clear audit trail for all digital records that are permanently deleted.

5.2 PHYSICAL RECORDS

Physical records that are no longer required must be destroyed in such a way that ensures the information they contain cannot be reconstructed or accessed by unauthorized individuals. The following procedures detail the proper methods for securely destroying physical records.

5.2.1 Shredding

Shredding is the preferred method for destroying paper records, as it ensures that the information is irreversibly fragmented. Peace by Youth (PY) will use cross-cut shredders, which cut paper into small, unrecognizable pieces. For large volumes of paper records, the organization may contract with a certified document destruction service to perform bulk shredding. A certificate of destruction should be obtained for each shredding event to confirm compliance.

5.2.2 Incineration

For certain sensitive documents, incineration may be an appropriate destruction method. Incineration ensures that documents are entirely reduced to ash, leaving no recoverable material. Incineration must take place in a controlled environment to prevent unauthorized access to the materials before they are destroyed.

5.2.3 Recycling

For non-confidential documents that do not contain sensitive or personal information, recycling may be an appropriate disposal method. However, care must be taken to ensure that records are sufficiently altered or shredded before recycling to prevent the unauthorized recovery of information.

5.2.4 Disposal of Non-Paper Physical Records

Other types of physical records, such as CDs, DVDs, or other media containing sensitive information, must also be destroyed in a secure manner. This may involve shredding the discs, cutting them into pieces, or incinerating them. Electronic devices such as hard drives or flash drives should be disposed of following the guidelines outlined in the **Digital Records** section.

5.2.5 Physical Disposal Records

A **Physical Disposal Record** must be maintained for all physical records that are destroyed. This record should include the document name, reference code, document category, destruction date, and the method of destruction. If third-party destruction services are used, a certificate of destruction must be attached to the disposal record.

5.3 DISPOSAL PROCEDURES AND ACCOUNTABILITY

Peace by Youth (PY) is committed to ensuring that the destruction of documents is conducted in a secure and accountable manner. The following steps outline the disposal procedures and the responsibilities of individuals involved in document destruction:

5.3.1 Document Review Before Destruction

Before a document is destroyed, it must be reviewed by the relevant department to confirm that its retention period has expired and that it is no longer required for operational, legal, or historical purposes. In cases where documents may be subject to litigation holds or regulatory investigations, their destruction should be postponed until the matter is resolved.

5.3.2 Approval for Destruction

For sensitive or high-risk documents, approval for destruction must be obtained from the department head or another designated authority. This ensures that the destruction process is properly supervised and that no critical records are accidentally destroyed.

5.3.3 Destruction Accountability

All document destruction activities must be documented, and an accountability trail must be maintained to ensure compliance with this policy. A dedicated **Records Manager** or other designated individual is responsible for overseeing the destruction process and ensuring that proper disposal records are maintained. Regular audits should be conducted to confirm compliance with document destruction protocols.

6. RESPONSIBILITIES

The effective implementation of the Document Retention and Management Policy requires the collective effort of all personnel involved in creating, maintaining, and disposing of records. Specific responsibilities have been designated to ensure that this policy is applied consistently and that Peace by Youth (PY) remains compliant with legal, regulatory, and operational requirements. The following roles outline the key responsibilities for managing records at Peace by Youth (PY).

6.1 RECORDS MANAGER

The Records Manager holds a central role in the administration and oversight of the Document Retention and Management Policy. This individual is responsible for ensuring that the organization's document retention practices are aligned with the requirements outlined in this policy and that documents are managed in a secure, efficient, and compliant manner.

Key Responsibilities:

- **Policy Implementation**: Ensure that the Document Retention and Management Policy is consistently applied across all departments and that all personnel are aware of their responsibilities.
- **Training and Guidance**: Provide training and guidance to department heads and staff regarding document retention, storage, and destruction procedures. The Records Manager must ensure that all staff understand their role in maintaining proper record-keeping practices.
- **Access Control**: Oversee access to sensitive documents and ensure that appropriate measures are in place to restrict access to authorized personnel only. This includes managing permission settings for digital records and controlling physical access to sensitive files.
- **Retention Monitoring**: Monitor the retention periods of all documents and ensure that records are not retained longer than necessary unless subject to a legal hold or specific regulatory requirement.
- **Document Disposal Oversight**: Supervise the secure disposal of documents that have reached the end of their retention period. The Records Manager is responsible for ensuring that all destruction is carried out in accordance with the security protocols outlined in this policy.
- **Incident Response**: Address any incidents of unauthorized access, data breaches, or non-compliance with the document retention policy. The Records Manager must ensure that appropriate actions are taken to mitigate risks and report incidents to senior management.
- **Auditing and Reporting**: Conduct regular audits of document retention practices across all departments to ensure compliance with this policy. The Records Manager will report audit findings to the Board of Directors and make recommendations for improvements if necessary.
- **Documentation**: Maintain records of document destruction activities, including certificates of destruction from third-party service providers. The Records Manager must ensure that proper records are kept for all document disposal events, including details on the document category, date of destruction, and method used.

6.2 DEPARTMENT HEADS

Department heads are responsible for ensuring that the Document Retention and Management Policy is effectively implemented within their respective departments. They must work closely with the Records Manager to ensure that their teams are adhering to the document retention guidelines and that proper record-keeping practices are maintained.

Key Responsibilities:

- **Policy Compliance**: Ensure that all staff within their department comply with the Document Retention and Management Policy. This includes ensuring that records are retained for the appropriate time and disposed of securely when no longer needed.
- **Record-Keeping Oversight**: Monitor the creation, storage, and use of documents within their department to ensure that they align with the guidelines set forth in this policy. Department heads should ensure that staff are following proper protocols for document storage, security, and accessibility.
- **Coordination with Records Manager**: Coordinate with the Records Manager to ensure that retention schedules are followed, and documents are disposed of appropriately. Department heads are responsible for notifying the Records Manager when documents in their department are due for disposal.
- **Incident Reporting**: Report any issues or incidents related to document retention, including loss of records, unauthorized access, or non-compliance with this policy. Department heads are responsible for ensuring that any breaches are reported promptly and addressed appropriately.
- **Training**: Ensure that staff within the department receive adequate training on the document retention policy and understand their responsibilities in managing records.

6.3 ALL EMPLOYEES

All employees play a role in maintaining the integrity of Peace by Youth's (PY) document retention practices. Whether directly involved in creating records or responsible for maintaining them, each employee must adhere to the guidelines outlined in this policy to ensure compliance with legal and operational standards.

Key Responsibilities:

- **Policy Adherence**: Employees must follow the document retention and management guidelines as established in this policy. This includes understanding the retention periods applicable to their work and ensuring that records are properly stored and managed.
- **Confidentiality and Security**: Employees are responsible for maintaining the confidentiality and security of records they handle, especially sensitive or confidential documents. Access to records should be limited to authorized personnel only, and any breaches must be reported immediately.
- **Document Creation and Filing**: Employees must ensure that records are accurately created, labeled, and filed according to the organization's filing system. Proper labeling and organization are essential for ensuring that records can be easily retrieved when needed.
- **Record Disposal**: Employees must follow the proper procedures for the secure disposal of records that have reached the end of their retention period. This includes adhering to the guidelines for digital and physical document destruction outlined in the policy.
- **Reporting Issues**: Employees must report any issues related to document retention, such as accidental deletion, loss of records, or unauthorized access, to their supervisor or the Records Manager. Prompt reporting is critical for addressing issues and mitigating risks.

7. POLICY REVIEW AND UPDATES

The Document Retention and Management Policy is a living document that must evolve in response to changing legal, regulatory, and operational requirements. Regular review and updates of this policy are essential to ensure that Peace by Youth (PY) remains compliant with applicable laws and continues to follow best practices for document management.

7.1 ANNUAL REVIEW

This policy will be reviewed annually by the Records Manager in collaboration with department heads and other relevant stakeholders. The purpose of the review is to assess the effectiveness of the current document retention practices and to determine whether any updates or modifications are needed based on changes in:

- **Legal and Regulatory Requirements**: Laws and regulations governing document retention and data protection are subject to change. The annual review will ensure that the policy is updated to reflect any new legal obligations or compliance requirements.
- **Organizational Needs**: As Peace by Youth (PY) grows and evolves, its operational needs may change. The policy review process will assess whether the current retention schedules, storage practices, and security measures remain appropriate given the organization's size, structure, and strategic priorities.
- **Technology Advancements**: Advancements in technology may impact the way documents are stored, accessed, and destroyed. The policy will be reviewed to ensure that it reflects the latest best practices in digital document management and data security.
- **Incident History**: Any incidents of non-compliance, data breaches, or unauthorized access will be taken into account during the policy review process. The review will identify potential gaps in the current policy and recommend improvements to prevent future incidents.

7.2 RECOMMENDATIONS FOR UPDATES

Following the annual review, the Records Manager will prepare a report outlining any recommendations for updates to the policy. The report will include:

- **Findings** from the review process, including any areas where the current policy may be insufficient or outdated.
- **Recommended Changes** to retention schedules, access controls, storage practices, or disposal procedures based on changes in legal requirements, technology, or organizational needs.
- **Action Plans** for implementing the recommended changes, including any necessary training or system updates.

7.3 APPROVAL OF UPDATES

Any proposed changes to the Document Retention and Management Policy must be approved by the Board of Directors before they are implemented. The Records Manager will present the proposed updates to the board for review and approval. Once approved, the updated policy will be communicated to all employees, and any necessary training will be provided to ensure that the new guidelines are understood and followed.

7.4 COMMUNICATION OF POLICY UPDATES

Once approved, updates to the policy must be communicated clearly to all employees, board members, and volunteers. This communication may take place through:

- **Email Notifications**: All staff will be informed of the changes via email, with a copy of the updated policy attached for reference.
- **Training Sessions**: If the updates involve significant changes to procedures or retention requirements, mandatory training sessions will be conducted to ensure that all personnel understand the new guidelines.

- **Internal Documentation**: The updated policy will be reflected in all internal documentation and record-keeping systems, ensuring consistency across the organization.

7.5 INTERIM UPDATES

While an annual review is the standard, interim updates to the policy may be required if there are significant changes in laws, regulations, or organizational operations. The Records Manager is responsible for identifying when an interim update is necessary and initiating the approval process with the Board of Directors.

The success of Peace by Youth's (PY) Document Retention and Management Policy relies on the collaboration of all employees, from the Records Manager overseeing the policy to each staff member following the established guidelines. By adhering to the responsibilities outlined in this section and regularly reviewing and updating the policy, Peace by Youth (PY) ensures compliance, efficiency, and the security of its organizational records.