Jamaica Union Conference
DATA PROTECTION POLICY
(May 2024)

A. Introduction

The Jamaica Union Conference of Seventh-day Adventists and its affiliated entities (hereafter collectively referred to as JAMU) require the collection and use of specific information about individuals. These individuals may include but are not limited to, stakeholders, volunteers, church members, suppliers, employees, or any other persons with whom the organization interacts or may need to communicate.

This policy outlines the procedures for collecting, handling, and storing personal data to ensure adherence to JAMU's data protection standards and compliance with Jamaica's Data Protection Act (2020).

B. Purpose

This data protection policy ensures that the JAMU:

1. Complies with data protection laws and adheres to best practices.
2. Protects the rights of individuals whose information is collected and processed.
3. Maintains transparency about how personal data is stored and processed.
4. Safeguards itself against the risks associated with data breaches.

C. The Data Protection Act (DPA)

The Data Protection Act (DPA) outlines the requirements for how organizations, including the JAMU, must collect, handle, and store personal information. These regulations apply regardless of whether the data is stored electronically, on paper, or in other formats. To comply with the law, personal information must be collected and used fairly, stored securely, and not disclosed unlawfully.

The DPA is based on eight key principles, which are as follows:

1. **Fairness and Lawfulness:** Personal data must be processed fairly and lawfully and must not be obtained by deception or any misleading information.
2. **Purpose Limitation:** Personal data must only be obtained for a specific and lawful purpose and must not be processed in any manner incompatible with those purposes.
3. **Data Minimization:** Personal data must be adequate, relevant and must be limited to what is necessary in relation to the purposes for which they are processed.
4. **Accuracy:** Personal data must be accurate and, where necessary, kept up to date;
5. **Storage Limitation:** Personal data must not be kept for longer than is necessary and must be disposed of in accordance with any regulations (once passed) under the Act.
6. **Rights of the Data Subject:** Personal data must be processed in accordance with the rights of the data subject. Some of these rights include the right to access the data and the right to prevent processing of the data in certain specified circumstances.
7. **Implementation of Technical and Organizational Measures:** Personal data must be protected using appropriate technical and organizational measures so as to prevent unauthorized or unlawful processing of the data as well as any accidental loss or destruction of, or damage to, the data.

8. **Cross-Border Transfers:** Personal data shall not be transferred to a State or territory outside of Jamaica unless that State or territory ensures an adequate level of protection for the rights and freedoms of the data subjects in relation to the processing of personal data.

D. Scope

This policy applies to:

1. The administrative offices of the JAMU.
2. All Seventh-day Adventist churches within JAMU's territory.
3. All staff and volunteers of the JAMU and its affiliated entities.
4. All individuals working on behalf of the JAMU and its affiliated entities.
5. All data that is held by the JAMU and its affiliated entities, that pertains to identifiable individuals.

E. Data Protection Risks

This policy helps to protect JAMU from various data security risks, including:

- **Breaches of confidentiality:** For instance, information being disclosed inappropriately.
- **Failure to offer choice:** Ensuring that all individuals have the freedom to decide how their data is used by the organization.
- **Reputational damage:** For example, JAMU's reputation could be harmed if hackers gain access to sensitive data.

F. Responsibilities

Everyone who works for or with JAMU has a responsibility to ensure that data is collected, stored, and handled properly. Each department that deals with personal data must ensure it is managed and processed in accordance with this policy and data protection principles.

The JAMU Executive Committee holds ultimate responsibility for ensuring that JAMU meets its legal obligations. However, there are specific responsibilities assigned as follows:

The **Data Protection Officer (DPO)**, through the office of the Secretariat, is responsible for:

- Keeping the board informed about data protection responsibilities, risks, and issues.
- Reviewing all data protection procedures and related policies according to an agreed schedule.
- Organizing data protection training and providing advice for individuals covered by this policy.
- Addressing data protection questions from staff, members, and others covered by this policy.
- Handling requests from individuals to access the data the organization holds about them (also known as 'subject access requests').
- Reviewing and approving any contracts or agreements with third parties that may involve handling the organization's sensitive data.

The **IT Manager** is responsible for:

- Ensuring that all systems, services, and equipment used for storing data comply with acceptable security standards.
- Conducting regular checks and scans to ensure that security hardware and software are functioning correctly.
- Assessing any third-party services the organization is considering for data storage or processing, such as cloud computing services, social media, or other communication platforms.

The **Communication director** is responsible for:

- Approving any data protection statements included in communications such as emails and letters.
- Handling any data protection inquiries from journalists or media outlets, including newspapers.
- Collaborating with other staff, when necessary, to ensure that marketing initiatives comply with data protection principles.

G. Office Staff Guidelines

- Access to data covered by this policy is restricted to individuals who require it to perform their job duties.
- Data should not be shared informally. Employees needing access to confidential information must request it through their supervisors or line managers.
- The JAMU will provide comprehensive training to all employees to ensure they understand their responsibilities when handling data.
- Employees must secure all data, by taking appropriate precautions and adhering to the guidelines outlined in this policy.
- Strong passwords must be utilized, changed frequently, and never shared.
- Personal data should not be disclosed to unauthorised individuals, whether within the organisation or externally.
- Data should be regularly reviewed and updated to ensure accuracy. Data that is no longer relevant, should be deleted and disposed of.
- Employees should seek guidance from their supervisor or the DPO if they have any questions or uncertainties regarding data protection.

H. Data Storage

The following rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager. When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees/Volunteers should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.
- When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts.
- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a memory stick), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing service.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. These backups should be tested regularly.
- Data should never be saved directly to laptops or other mobile devices like tablets or smartphones.
- All servers and computers containing data should be protected by approved security software

and a firewall.

I. Data Use

JAMU places value on personal data only when it serves the organisation's charitable goals. Yet, the greatest risks to personal data occur when it is accessed and utilized. Therefore:

- Employees must ensure that their computer screens are locked when unattended while handling personal data.
- Informal sharing of personal data is prohibited; email is an insecure means of sharing such information.
- All data must be encrypted before electronic transfer; guidance on secure data transfer is available from the IT manager.
- Personal data should not be transferred outside Jamaica unless approved by the Office of the Information Commissioner.
- Employees are advised against saving personal data on personal devices; the central data copy should be accessed and updated at all times.

J. Data Accuracy

The law requires the JAMU to take reasonable steps to ensure data is kept accurate and up to date. It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up-to-date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a member's details when they call.
- The JAMU will make it easy for data subjects to update the information the JAMU holds about them.
- Data should be updated as and when inaccuracies are discovered. For instance, if a member can no longer be reached on their stored telephone number, it should be removed from the database at that time.

K. Subject Access Requests

Every individual whose personal data is held by the JAMU has the right to:

- Inquire about the information the organization holds about them and the reasons for its retention.
- Seek guidance on accessing this information.
- Receive instructions on how to keep their data current.
- Learn about the JAMU's compliance with data protection regulations.

When an individual contacts the JAMU to request this information, it constitutes a 'subject access request'. Such requests should be submitted via email to the JAMU. The information must be provided free of charge, although a reasonable fee may apply in cases of clearly unjustified or excessive requests, especially if they are repetitive. The JAMU is required to furnish the pertinent data promptly and no later than one month after receiving the request. The JAMU will always confirm the identity of the requester before disclosing any information in response to a subject access request.

L. Disclosing Data for Other Reasons

Under specific conditions, the DPA permits the disclosure of personal data to law enforcement agencies without the data subject's consent. In such situations, the JAMU will verify the legitimacy of the request, seeking guidance from the trustees and legal advisors of the organization as needed.

M. Providing Information

The JAMU strives to inform individuals about the processing of their data, ensuring they comprehend how their data is utilized and how to assert their rights. To achieve these objectives, the JAMU provides privacy statements that detail the utilization of individuals' data by the JAMU.

N. Privacy Notice (employees)

We process the personal data of individuals employed or otherwise engaged as part of our workforce. This is done for employment purposes, to facilitate the organization's operations, and to ensure that individuals receive their remuneration.

The personal data we process may include, but may not be limited to, the following:

- **Identity Information**: This includes your name, date of birth, gender, photographs, passport details, National Insurance Number, nationality, marital status, and dependents.
- **Contact Information:** This includes your business and home addresses, telephone numbers, email addresses, and emergency contact details.
- **Employment Details:** This includes your position, terms of employment, performance and disciplinary records, and information on sickness and holidays.
- **Background Information:** This includes your CV, previous experience, qualifications, and certifications.
- **Financial Information:** This includes your bank details, tax information, salary, benefits, and expenses.
- **IT Information:** This includes information related to your access to our systems, such as login details, IP addresses, log files, access times, duration of use, and location.

Benefits of Collecting This Information:

- Improving the management of workforce data across the organization.
- Developing a comprehensive understanding of the workforce and its deployment.
- Informing the development of recruitment and retention policies.
- Enhancing financial modeling and planning.
- Ensuring compliance with our policies, procedures, and legal obligations.
- Monitoring selected protected characteristics.

Data Sharing:

We will not share your information with third parties without your consent unless legally permitted or required to do so.

Your Rights Under the DPA:

- Object to the processing of personal data that is likely to cause, or is causing, damage or distress.
- Prevent processing for the purpose of direct marketing.
- Object to decisions being taken by automated means.

- In certain circumstances, have inaccurate personal data rectified, blocked, erased, or destroyed.
- Claim compensation for damages caused by a breach of data protection legislation.

Further Information:

For more information about our data retention policy, how we use your personal data, or to request a copy of the information we hold about you, please contact the JAMU Executive Secretary at the JAMU Office, Manchester Road, Mandeville. Phone: (876) 656 8481.

If you have concerns about how we collect or use your personal data, you should initially raise them with the JAMU Executive Secretary or directly with the Office of the Information Commissioner at: https://oic.gov.jm/form/report-a-data-breach

O. Privacy Notice (non-employees)

1. Your personal data – what is it?

   Personal data, according to the Data Protection Act (2018), refers to any information that relates to an identified or identifiable individual. This can include data such as name, biometrics, location, identification numbers (TRN, NIS, etc.), and health information, among others.

2. Who are we?

   The Jamaica Union Conference of Seventh-day Adventists (JAMU) is the data controller (contact details below). This means it determines the purposes and means of processing personal data. In simpler terms, it is responsible for deciding why and how personal data is collected and processed.

   How do we process your personal data?

   The JAMU adheres to its obligations under the Data Protection Act (DPA) by maintaining accurate and up-to-date personal data, securely storing and disposing of data, and avoiding collecting or retaining excessive data. Additionally, we safeguard personal data against loss, misuse, unauthorized access, and disclosure. We also ensure that appropriate technical measures are implemented to protect personal data.

   We use your personal data for the following purposes:

   - To enable us to provide a voluntary service for the benefit of the public in a particular geographical area (for example church events and community programs) as outlined in our constitution;
   - To manage membership records;
   - To raise funds, receive donations, and promote the interests of the organization;
   - To manage our employees and volunteers;
   - To maintain our accounts and records;
   - To inform you of news, events, activities, and services running within the JAMU;

3. What is the legal basis for processing your personal data?

   - Explicit consent of the data subject allowing us to keep you informed about news, events, activities and services and process your donations and keep you informed.
   - Processing is necessary for carrying out obligations under employment, National Insurance Scheme (NIS), or social protection law, or in accordance with a collective agreement.

4. Sharing your personal data

   Your personal data will be treated with strict confidentiality and will only be shared with other church members to provide services to fellow members or for church-related purposes. We will only share your data with third parties outside of JAMU with your explicit consent.

5. How long do we keep your personal data?

   We keep data only as long as it is needed, in accordance with the guidance set out in JAMU's Data Retention Policy

6. Your rights and your personal data

   Unless subject to an exemption under the DPA, you have the following rights with respect to your personal data:

   - The right to request a copy of your personal data which the JAMU holds about you;
   - The right to request that the JAMU corrects any personal data if it is found to be inaccurate or out of date;
   - The right to request your personal data is erased where it is no longer necessary for the JAMU to retain such data;
   - The right to withdraw your consent to the processing at any time
   - The right to request that the JAMU provide the data subject with his/her personal data and where possible, to transmit that data directly to another data controller.
   - The right, where there is a dispute concerning the accuracy or processing of your personal data, to request a restriction is placed on further processing;
   - The right to object to the processing of personal data, where applicable.
   - The right to lodge a complaint with the Office of the Information Commissioner.

7. Further processing

8. If we intend to use your personal data for a purpose not outlined in this Data Protection Notice, we will inform you about the new use before starting the processing. This new notice will detail the specific purposes and conditions for processing. When required, we will obtain your prior consent for the new use of your data.

9. Contact Details

   To exercise all relevant rights, or to submit queries or complaints, please in the first instance contact the JAMU Executive Secretary, JAMU Office, Manchester Road, Mandeville. Phone: (876) 656-8481.

   You can contact the Office of the Information Commissioner as follows:

   - Phone: (876) 929-8568, (876) 929-6952, (876) 960-0874, (876) 968-5622
   - Email: i n f o @ o i c . g o v . j m
   - Address: Masonic Building, 2nd Floor, 45 – 47 Barbados Avenue Kingston 5

P. DATA RETENTION POLICY

1. Employee Data

   Our goal is to retain employee data only for as long as necessary for the purposes for which it is processed. The table below outlines the retention periods for the employee data we may hold.

   Certain personal data is kept for employment purposes, to support the organization's operations, and/or to facilitate payment to individuals. In these cases, we generally adhere to the 'recommended' retention period. Other personal data is retained to comply with statutory

requirements, in which case we follow the 'statutory' retention period.

Record	Retention period
Accident books, accident records, accident reports	Three years from the date of the last entry (or, if the accident involves a child/ young adult, then until that person reaches age 21). Statutory.
Accounting records	Three years for private companies, six years for public limited companies. Statutory.
Actuarial valuation reports	Permanently. Recommended.
Application forms and interview notes (for unsuccessful candidates)	Six months. Recommended.
Assessments under health and safety regulations and records of consultations with safety representatives and committees	Permanently. Recommended.
Driving licence, vehicle insurance, MOT certificate details	One year after expiry unless renewed. Recommended.
Expatriate records and other records relating to foreign employees (e.g. visa, work permits, etc.	Six years after employment ceases. Recommended.
National minimum wage records	Three years after the end of the pay reference period following the one that the records cover. Statutory.
Parental leave records	Five years from birth/adoption of the child or 18 years if the child receives a disability living allowance. Recommended.
Pensioners' records	12 years after benefit ceases. Recommended.
Personnel files and training records (including disciplinary records and working time records)	Six years after employment ceases. Recommended.
Records relating to children and young adults	Until the child/young adult reaches age 18. Statutory.
Redundancy details, calculations of payments, refunds.	Six years from the date of redundancy. Recommended.
Retirement Benefits Schemes – records of notifiable events, for example, relating to incapacity	Six years from the end of the scheme year in which the event took place. Statutory.
Trust deeds and rules	Permanently. Recommended.
Trustees' minute books	Permanently. Recommended.
Wage/salary records (also overtime, bonuses, expenses)	Six years. Statutory.
Working time records	Two years from date on which they were made. Statutory.
Baptismal Records	Permanently. Recommended

Marriage Records	Permanently. Recommended
Membership Records	Permanently. Recommended
Donations, Tithe and Offering Records	Seven years. Statutory.
Church Meeting Minutes	Permanently. Recommended
Volunteer Records	Six years after the volunteer ceases their role. Recommended.
Event Records	Three years after the event. Recommended.
Insurance Policies	Seven years after the policy expires. Statutory.
Property Records	Permanently. Recommended.
Service Records	Permanently. Recommended.

The retention guidance for additional denominational records is found in the General Conference Model Retention Schedule July 2015, published by the General Conference Office of Archives, Statistics, and Research (ASTR).

https://www.adventistarchives.org/retention-schedule.pdf