BUC Policy - Section 10

DATA PROTECTION POLICY

(revised Mar 2018)

A. Introduction (revised Mar 2018)

The British Union Conference of Seventh-day Adventists together with its constituent entities (henceforth referred to collectively as the BUC), needs to gather and use certain information about individuals. These individuals can include interests, volunteers, church members, suppliers, employees, or other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the BUC's data protection standards and to comply with the law.

B. Purpose (revised Mar 2018)

This data protection policy ensures that the BUC:

1. complies with data protection law and follows good practice
2. protects the rights of those whose information is held and processed
3. is open about how it stores and processes individuals' data
4. protects itself from the risks of a data breach

C. General Data Protection Regulation (GDPR) (revised Mar 2018)

GDPR describes how organisations, including the BUC, must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

GDPR is underpinned by six important principles. These say that personal data must be:

1. processed lawfully, fairly and in a transparent manner in relation to the data subject;
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. accurate and, where necessary, kept up to date; inaccurate or outdated personal data should be deleted or rectified without delay;
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

D. Scope (revised Mar 2018)

This policy applies to:

1. The administrative offices of the BUC.
2. All Seventh-day Adventist churches within the territory of the BUC.
3. All staff and volunteers of the BUC and its constituent entities.

4. All people working on behalf of the BUC and its constituent entities.

5. All data that is held by the BUC and its constituent entities, relating to identifiable individuals

E. Data Protection Risks (revised Mar 2018)

This policy helps to protect the BUC from some data security risks, including:

- Breaches of confidentiality. For example, information being given out inappropriately.
- Failing to offer choice. For examples, all individuals should be free to choose how the organisation uses data relating to them.
- Reputational damage. For example, the BUC could suffer if hackers successfully gained access to sensitive data.

F. Responsibilities (revised Mar 2018)

Everyone who works for or with the BUC has some responsibility for ensuring that data is collected, stored and handled appropriately. Each department that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

The BUC Executive Committee is ultimately responsible for ensuring that the BUC meets its legal obligations. However, there are specific responsibilities, as follows:

Secretariat is responsible for:

- Keeping the board updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from staff, members, and anyone else covered by this policy.
- Dealing with requests from individuals to see the data the organisation holds about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the organisation's sensitive data.

The IT director is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services the organisation is considering using to store or process data. For instance, cloud computing services, social media, or other communication platforms.

The Communication director is responsible for:

- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like newspapers.
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

G. Office Staff Guidelines (revised Mar 2018)

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- The BUC will provide training to all employees to help them understand their responsibilities when handling data.

- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used, frequently changed, and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the organisation or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their line manager or Secretariat if they are unsure about any aspect of data protection.

H. Data Storage (revised Mar 2018)

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 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 smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.

I. Data Use (revised Mar 2018)

Personal data is of no value to the BUC unless the BUC can use it to achieve the organisation's charitable objectives. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft. Therefore:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. It should never be sent by email, as this form of communication is not secure.
- Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorised external contacts.
- Personal data should never be transferred outside of the European Economic Area unless the country has been approved by the Information Commissioner's' Office.
- Employees should not save copies of personal data to their own computers. They should always access and update the central copy of any data.

J. Data Accuracy (revised Mar 2018)

The law requires the BUC 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 BUC will make it easy for data subjects to update the information the BUC holds about them. For instance, via the BUC website.
- 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 (revised Mar 2018)

All individuals who are the subject of personal data held by the BUC are entitled to:

- Ask what information the organisation holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the BUC is meeting its data protection obligations.

If an individual contacts the BUC requesting this information, this is called a subject access request. Subject access requests from individuals should be made by email, addressed to the BUC. The information must be provided free of charge, though a reasonable fee may be charged when a request is manifestly unfounded or excessive, particularly if it is repetitive. The BUC must provide the relevant data information without delay and at the latest within one month of receipt. The BUC will always verify the identity of anyone making a subject access request before handing over any information.

L. Disclosing Data for Other Reasons (revised Mar 2018)

In certain circumstances, the GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. In these circumstances, the BUC will ensure the request is legitimate, seeking assistance from the trustees and from the organisation's legal advisers where necessary.

M. Providing Information (revised Mar 2018)

The BUC aims to ensure that individuals are aware that their data is being processed, and that they understand how the data is being used and how to exercise their rights. To these ends, the BUC has privacy statements, setting out how data relating to individuals is used by the BUC.

N. Privacy Notice (employees) (revised Mar 2018)

We process personal data relating to those we employ to work as, or are otherwise engaged to work as, part of our workforce. We do this for employment purposes, to assist in the running of the charity and/or to enable individuals to be paid.

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

- data relating to your identity (including name, data of birth, gender, photographs, passport, National Insurance Number, immigration status, marital status, dependants),
- contact details (business and home address, telephone numbers, email addresses, emergency contact details),
- employment details (position, office location, terms of employment, performance and disciplinary records, sickness and holidays),

- background information (CV, previous experience, qualifications and certifications, criminal records check (for vetting purposes, where permissible and in accordance with applicable law),
- financial information (bank details, tax information, salary, benefits, expenses),
- IT information – information related to your access to our systems (login details, IP addresses, log files, access/times/duration of use, location).

The collection of this information will benefit us by:

- improving the management of workforce data across the business,
- enabling development of a comprehensive picture of the workforce and how it is deployed,
- informing the development of recruitment and retention policies,
- allowing better financial modelling and planning,
- ensuring compliance with our policies and procedures and our legal obligations,
- enabling monitoring of selected protected characteristics.

We will not share information about you with third parties without your consent unless the law allows or requires us to do so.

Under the data protection legislation you have the right to:

- object to 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 the data protection legislation.

If you would like to find out more about our data retention policy and how we use your personal data, or if you want to see a copy of the information about you that we hold, please contact the BUC Executive Secretary, BUC Office, Stanborough Park, WATFORD, WD25 9JZ. Phone: 01923 672251.

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with the BUC Executive Secretary in the first instance, or directly with the Information Commissioner's Office at: https://ico.org.uk/concerns

O. Privacy Notice (non-employees) (revised Mar 2018)

1. Your personal data – what is it?

Personal data relates to a living individual who can be identified from that data. Identification can be by the information alone or in conjunction with any other information in the BUC's possession or likely to come into such possession. The processing of personal data is governed by the General Data Protection Regulation (GDPR 2018).

2. Who are we?

The British Union Conference of Seventh-day Adventists (BUC) is the data controller (contact details below). This means it decides how your personal data is processed and for what purposes.

3. How do we process your personal data?

The BUC complies with its obligations under the GDPR by keeping personal data up to date; by storing and destroying it securely; by not collecting or retaining excessive amounts of data; by protecting personal data from loss, misuse, unauthorised access and disclosure, and by ensuring that appropriate technical measures are in place 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 programmes) as specified in our constitution;
- To administer membership records;

- To fundraise, receive donations, and promote the interests of the charity;
- To manage our employees and volunteers;
- To maintain our own accounts and records (including the processing of gift aid applications);
- To inform you of news, events, activities and services running within the BUC;

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

- Explicit consent of the data subject so that we can keep you informed about news, events, activities and services and process your gift aid donations and keep you informed.
- Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement.
- Processing is carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided:
  - i) the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes); and
  - ii) there is no disclosure to a third party without consent.

5. Sharing your personal data

Your personal data will be treated as strictly confidential and will only be shared with other members of the church in order to carry out a service to other church members or for purposes connected with the church. We will only share your data with third parties outside of the BUC with your consent.

6. 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 BUC's Data Retention Policy

7. Your rights and your personal data

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

- The right to request a copy of your personal data which the BUC holds about you;
- The right to request that the BUC 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 BUC to retain such data;
- The right to withdraw your consent to the processing at any time
- The right to request that the BUC 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 in relation to 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 Information Commissioners Office.

8. Further processing

If we wish to use your personal data for a new purpose, not covered by this Data Protection Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing.

9. Contact Details

To exercise all relevant rights, or to submit queries or complaints, please in the first instance contact the BUC Executive Secretary, BUC Office, Stanborough Park, WATFORD, WD25 9JZ. Phone: 01923 672251.

You can contact the Information Commissioners Office as follows:

- Phone: 0303 123 1113
- Email: https://ico.org.uk/global/contact-us/email
- Post: Information Commissioners Office, Wycliffe House, Water Lane, WILMSLOW, SK9 5AF.

P. DATA RETENTION POLICY (revised Mar 2018)

1. Employee Data

Our aim is to retain employee data for no longer than is necessary for the purposes for which the personal data is processed. The table below shows the retention periods for the employee data that we may hold.

Some personal data is retained for employment purposes, to assist in the running of the charity and/or to enable individuals to be paid, in which case we generally follow the 'recommended' retention period. Some personal data is retained for statutory purposes, in which case we follow the 'statutory' retention period.

This guidance has been supplied by our HR advice company, Citation.

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.
Control of Substances Hazardous to Health Regulations (COSHH) records of tests and examinations of control systems and protective equipment	Five years from the date on which the tests were carried out. Statutory.
DBS, PVG, AccessNI certificates/copies	Six months. Recommended.
DBS certificate information required by CQC	Three years or until superseded if less. 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.
Income tax and NI returns, income tax records and correspondence with HMRC	Not less than three years after the end of the financial year to which they relate. Statutory.
Inland Revenue/HMRC approvals	Permanently. Recommended.
Medical records and details of biological tests under the Control of Lead at Work Regulations	40 years from the date of the last entry. Statutory.
Medical records as specified by the Control of Substances Hazardous to Health Regulations (COSHH)	40 years from the date of the last entry. Statutory.
Medical records under the Control of Asbestos at Work Regulations, medical records containing details of employees exposed to asbestos and medical examination certificates	40 years from the date of the last entry (medical records); four years from the date of issue (medical examination certificates). Statutory.
Medical records under the Ionising Radiations Regulations 1999	Until the person reaches 75 years of age, but in any event for at least 50 years. Statutory.

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.
Pension scheme investment policies	12 years from the ending of any benefit payable under the policy. Recommended.
Pension scheme money purchase details	Six years after transfer or value taken. 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 21. Statutory.
Redundancy details, calculations of payments, refunds, notification to the Secretary of State	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.
Security Industry Authority (SIA) licence details	One year after expiry unless renewed. Recommended.
Senior executives' records (that is, those on a senior management team or their equivalents)	Permanently. Recommended.
SMP, SAP, SSPP records, calculations, certificates (Mat B1s) or other medical evidence, notifications, declarations and notices	Three years after the end of the tax year in which the leave period ends. Statutory.
Statutory Sick Pay records, calculations, certificates, self-certificates	Six years after the employment ceases. Recommended.
Time cards	Two years after audit. Recommended.
Trade union agreements	10 years after ceasing to be effective. Recommended.
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.
Works Council minutes	Permanently. Recommended.

2. Other BUC Data

The retention guidance for other denominational records is found in TED Working Policy BA 70, Retention and Safeguarding of Records, and the General Conference Model Retention Schedule July 2015, published by the General Conference Office of Archives, Statistics, and Research (ASTR).