Privacy Policy:

Data Protection Policy

Data Protection Legislation is concerned with the protection of human rights in relation to personal data. The aim of the Legislation is to ensure that personal data is used fairly and lawfully and that where necessary the privacy of individuals is respected. During the course of the activities of Keswick Ministries, Keswick Ministries will collect, store and process personal data about our supporters, people who attend our Convention & year round events, employees, suppliers and other third parties and we recognise that the correct and lawful treatment of this data will help maintain confidence in Keswick Ministries. This policy sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

The Data Protection Compliance Officer is responsible for ensuring compliance with the Legislation and with this policy. The post is held by Roz Lake, contactable by email: roz.lake@keswickministries.org or by phone 017687 80075.

Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Compliance Manager.

Processing personal data

All personal data should be processed in accordance with the Legislation and this policy. Any breach of this policy may result in disciplinary action.

Processing includes obtaining, holding, maintaining, storing, erasing, blocking and destroying data.
Personal data is data relating to a living individual. It includes employee data. It will not include data relating to a company or organisation, although any data relating to individuals within companies or organisations may be covered. Personal data can be factual (for example a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

Examples of personal data are employee details, including employment records, names and addresses and other information relating to individuals, including supplier details, any third-party data and any recorded information including any recorded telephone conversations, emails or CCTV images.

Employees and others (including contracted staff, volunteers and trustees) who process data on behalf of Keswick Ministries (referred to in this policy as ‘Employees’) should assume that whatever they do with personal data will be considered to constitute processing.

Employees should only process data:

If they have consent to do so;

or

If it is necessary to fulfil a contractual obligation or as part of the employer/employee relationship; for example, processing the payroll;

or

the processing is necessary for legitimate interests pursued by Keswick Ministries, unless these are overridden by the interests, rights and freedoms of the data subject.

If none of these conditions are satisfied, individuals should contact the Data Protection Compliance Manager before processing personal data.

Appendix

Appendix 1 - Information Security Policy

Information security involves preserving confidentiality, preventing unauthorised access and disclosure, maintaining the integrity of information, safeguarding accuracy and ensuring access to information when required by authorised users. In addition to complying with this policy, all users must comply with the Data Protection Legislation and the Data Protection Policy. 'Keswick Ministries data' means any personal data processed by or on behalf of Keswick Ministries. Information security is the responsibility of every member of staff, trustee, contractor & volunteer using Keswick Ministries data on but not limited to Keswick Ministries information systems. This policy is the responsibility of Roz Norris who will undertake supervision of the policy. Our IT systems may only be used for authorised purposes. We will monitor the use of our systems from time to time. Any person using the IT systems for unauthorised purposes may be subject to disciplinary and/or legal proceedings. We will take appropriate technical and organisational steps to guard against unauthorised or unlawful processing. In particular: All data will be stored in a secure location and precautions will be taken to avoid data being accidentally disclosed. Manual records relating to supporters or staff will be kept secure in locked cabinets. Access to such records will be restricted. Access to systems on which information is stored must be password protected with strong passwords and these should be changed at once if there is a risk they have been compromised. Passwords must not be disclosed to others. We will ensure that staff and members who handle personal data are adequately trained and monitored to ensure data is being kept secure. We will ensure that only those who need access will have access to data. We will take particular care of sensitive data and security measures will reflect the importance of keeping sensitive data secure (definition of sensitive data is set out above in the Data Protection Policy), e.g. password protection for documents and encryption. Where personal data needs to be deleted or destroyed adequate measures will be taken to ensure data is properly and securely disposed of. This will include destruction of files and back up files and physical destruction of manual files. Particular care should be taken over the destruction of manual sensitive data (written records) including shredding or disposing via specialist

contractors (who will be treated as data processors - see below). 2 We will ensure that any data processor engaged to process data on our behalf (e.g. for payroll) will act under a written contract and will give appropriate undertakings as to the security of data. Appropriate software security measures will be implemented and kept up to date. We will ensure that if information has to be transported or transferred, this is done safely using encrypted devices or services. Where personal devices are used to store or process personal data, they must be subject to appropriate security. All breaches of this policy must be reported to Roz Norris This policy will be regularly reviewed and audited. Policy adopted on 23 May 2018 To be reviewed in 12 months

Appendix 2 - Record Retention Policy with Guidelines

All data and records will be stored in accordance with the security requirements of the Data Protection Legislation and in the most convenient and appropriate location having regard to the period of retention required and the frequency with which access will be made to the record. 2. Data and records which are active should be stored in the most appropriate place for their purpose commensurate with security requirements. 3. Data and records which are no longer active, due to their age or subject, should be stored in the most appropriate place for their purpose or destroyed. 4. The degree of security required for file storage will reflect the sensitivity and confidential nature of any material recorded. 5. Any data file or record which contains personal data of any form can be considered as confidential in nature. 6. Data and records should not be kept for longer than is necessary. This principle finds statutory form in the Data Protection Legislation, which requires that personal data processed for any purpose "shall not be kept for longer than is necessary for that purpose". All staff, trustees, contractors & volunteers of Keswick Ministries are required to have regard to the Guidelines for Retention of Personal Data attached hereto. 7. Any data that is to be disposed of must be safely disposed of for example by shredding. Any group which does not have access to a shredder should pass material to Roz Norris who will undertake secure shredding. 8. Special care must be given to disposing of data stored in electronic media. Guidance will be given by Roz Norris to any group which has stored personal data relating to its members on for example personal computers which are to be disposed of. Policy adopted on 23 May 2018 To be reviewed in 12 months 2 Guidelines for Retention of Personal Data (This is not an exhaustive list) If you have any queries regarding retaining or disposing of data please contact Roz Norris Types of Data Suggested Retention Period Personnel files including training records and notes of disciplinary and grievance hearings. 6 years from the end of employment Application forms / interview notes Maximum of one year from the date of the interviews for those not subsequently employed. If employed, retain in personnel file. Information relating to children NB. You may find it helpful to read the following article: http://safeinchurch.org.uk/record-retention Check for accuracy with each donation/booking Record that child was a member of the youth/kids work – permanent Secure destruction of personal data other than name and fact of attendance – three years after ceasing to be an attendee Keswick Ministries Supporter

(inc. event participants) information Check for accuracy with each donation/booking Record that adult was a supporter – permanent Secure destruction of personal data other than name and previous contact and any legal records appropriate to giving – three years after cease to be a supporter Volunteer information Check for accuracy with each new application Record that adult was a volunteer – permanent Secure destruction of personal data (previous application forms & content) other than name and fact of volunteering – three years after ceasing to be a volunteer Income Tax and NI returns, including correspondence with tax office At least 6 years after the end of the financial year to which the records relate Statutory Maternity Pay records and calculations As Above (Statutory Maternity Pay (General) Regulations 1986) 3 Statutory Sick Pay records and calculations As Above Statutory Sick Pay (General) Regulations 1982 Wages and salary records 6 years from the tax year in which generated Accident books, and records and reports of accidents (for Adults) 3 years after the date of the last entry (for children) three years after the child attains 18 years (RIDDOR 1985) Health records 6 months from date of leaving employment (Management of Health and Safety at Work Regulations) Health records where reason for termination of employment is connected with health, including stress related illness 3 years from date of leaving employment (Limitation period for personal injury) claims)

Appendix 3 - Data Breach Procedure

Introduction Keswick Ministries (“we”) hold and process personal data which needs to be protected. Every care is taken to protect the data we hold. Compromise of information, confidentiality, integrity or availability may result in harm to individuals, reputational damage, detrimental effect on service provision, legislative non-compliance and financial penalties. Purpose This policy sets out the procedure to be followed to ensure a consistent and effective approach throughout the organisation. Scope The policy relates to all personal data held by Keswick Ministries, regardless of format. It applies to anyone who handles this personal data, including those working on behalf of the organisation. The objective of the policy is to contain any breaches, to minimise the risks associated with the breach and to consider what action is necessary to secure personal data and prevent any further breach. Types of breach An incident is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to data subjects. An incident includes but is not restricted to: Loss or theft of personal data or the equipment on which the data is stored e.g. laptop, memory stick, smartphone, or paper record Theft or failure of equipment on which personal data is stored Unauthorised use of or access to personal data Attempts to gain unauthorised access to personal data Unauthorised disclosure of personal data Website defacement Hacking attack 2 Reporting an incident Any person using personal data on behalf of Keswick Ministries is responsible for reporting data breach incidents immediately to Roz Norris (Data Protection Officer) or in her absence David Sawday (Chief of Operations). The report should contain the following details: Date

and time of discovery of breach Details of person who discovered the breach The nature of the personal data involved How many individuals' data is affected Containment and recovery Roz Norris will first ascertain if the breach is still occurring. If so, appropriate steps will be taken immediately to minimise the effects of the breach. An assessment will be carried out to establish the severity of the breach and the nature of further investigation required. Consideration will be given as to whether the police should be informed. Advice from appropriate experts will be sought if necessary. A suitable course of action will be taken to ensure a resolution to the breach. Investigation and risk assessment An investigation will be carried out without delay and where possible within 24 hours of the breach being discovered. Roz Norris will assess the risks associated with the breach, the potential consequences for the data subjects, how serious and substantial those are and how likely they are to occur. The investigation will take into account the following: The type of data involved and its sensitivity The protections in place (e.g. encryption) What has happened to the data Whether the data could be put to illegal or inappropriate use Who the data subjects are, how many are involved, and the potential effects on them Any wider consequences Notification Roz Norris will decide with appropriate advice who needs to be notified of the breach. Every incident will be assessed on a case by case basis. The Information Commissioner will be notified, if at all possible within 24 hours of the data breach, if a large number of people are affected or the consequences for the data subjects are very serious. Guidance on when and how to notify the ICO is available on their website https://ico.org.uk/fororganisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/ Where appropriate, we will notify the data subjects whose personal data has been affected by the incident; such a notification may include a description of how and when the breach 3 occurred, and the nature of the data involved, and specific and clear advice on what they can do to protect themselves and what has already been done to mitigate the risks. Roz Norris will keep a record of all actions taken in respect of the breach. Evaluation and response Once the incident is contained, Roz Norris will carry out a review of the causes of the breach, the effectiveness of the response, and whether any changes to systems, policies or procedures should be undertaken. Consideration will be given to whether any corrective action is necessary to minimise the risk of similar incidents occurring. Policy adopted on 23 May 2018 To be reviewed in 12 months' time

Appendix 4 - Complaints Process

Appendix 4 - Keswick Ministries Data Protection Complaints Process Keswick Ministries ("we") take your privacy concerns seriously. If you have any concerns about the way your information is being handled, please contact Roz Norris (Data Protection Officer) without delay. Roz can be contacted as follows: 017687 80075 roz.norris@keswickministries.org We will carefully investigate and review all complaints and take appropriate action in accordance with Data Protection Legislation. We will keep you informed of the progress of our investigation and the outcome. If you are not satisfied with the outcome, you may wish to contact the Information Commissioner's

Office at https://ico.org.uk/concerns/ Any complaint received by us must be referred to Roz Norris who will arrange for an investigation as follows: 1. A record will be made of the details of the complaint. 2. Consideration will be given as to whether the circumstances amount to a breach of Data Protection Legislation and action taken in accordance with the Data Breach Procedure. 3. The complainant will be kept informed of the progress of the complaint and of the outcome of the investigation. 4. At the conclusion of the investigation Roz Norris will reflect on the circumstances and recommend any improvements to systems or procedures.

How we use Web Cookies

A cookie is a small file which asks permission to be placed on your computer's hard drive. Once you agree, the file is added and the cookie helps analyze web traffic or lets you know when you visit a particular site. Cookies allow web applications to respond to you as an individual. The web application can tailor its operations to your needs, likes and dislikes by gathering and remembering information about your preferences.

Overall, cookies help us provide you with a better website, by enabling us to monitor which pages you find useful and which you do not. A cookie in no way gives us access to your computer or any information about you, other than the data you choose to share with us.

You can choose to accept or decline cookies. Most web browsers automatically accept cookies, but you can usually modify your browser setting to decline cookies if you prefer. This may prevent you from taking full advantage of the website.

There are two types of cookie you may encounter when using this website:

First party cookies

These are our own cookies, controlled by us and used to provide information about usage of our site.

Name	Purpose	Typical Content	Expires
ci_session	Authentication session to preserve any sign ins and other changes you might have made during your visit to this site.	Hashed data referring to your unique visit. No personal information unless signed in.	On exit
cookie_notice	Used to supress the cookie notice once the user opts to hide it	"Yes" or "No"	31 days, updated with each visit
prefixed with X-Mapping-	Set by our webserver to manage content	Information about which server is	On exit

	delivery on cloud based servers	providing content to the user	

Third party cookies

These are cookies found in other companies' internet tools which we are using to enhance our site, for example Facebook or Twitter have their own cookies, which are controlled by them.

Provider	Name	Purpose	More Info.
Google Analytics	Multiple cookies prefixed with __utm	These cookies are used to collect information about how visitors use our site. We use the information to compile reports and to help us improve the site. The cookies collect information in an anonymous form, including the number of visitors to the site, where visitors have come to the site from and the pages they visited.	Google Privacy policy
YouTube	VISITOR_INFO1_LIVE, PREF	YouTube embedded video	Google Policies and Principles
Vimeo	Multiple cookies prefixed with __utm and with domain .player.vimeo.com	Vimeo embedded video	Vimeo Privacy policy

Links to other websites

Our website contains links to other websites of interest. However, once you have used these links to leave our site, you should note that we do not have any control over that other website. Therefore, we cannot be responsible for the protection and privacy of any information which you provide whilst visiting such sites and such sites are not governed by this privacy statement. You should exercise caution and look at the privacy statement applicable to the website in question.