

**Data Protection, Security and Retention Policy**

Decisions for Trustees:

1. Appoint a Data Protection Officer or Compliance Officer to oversee the implementation and monitoring this policy. They would also take on some responsibilities this policy delegates to Office Manager.
   1. This will probably include writing handbooks and providing or organising training.
   2. One of the first tasks will be to audit what currently happens and propose a project plan to consolidate and move to being fully compliant.
2. Set up a Google or Microsoft free charity account for email, cloud-based file storage and back up.
3. Do we have/need an IT Officer to oversee the various IT related issues?
4. These roles could be shared by more than 1 person. Would this be more effective?
5. Provide Camp Leaders with an external storage device with security software.
6. Provide camp leaders with a locakable file box.
7. Do we have any other concerns regarding security of data on camps? How can we mitigate against these risks?
8. Do we want a separate WYOD (Wear Your Own Device) Policy? I recommend to NOT have a policy, but to write these types of dev ices into this policy.
9. Clarify which responsibilities should remain with Trustees.
10. How do we ensure ALL volunteers know the policy and guidance and monitor compliance

**Contents**

1. Introduction
2. The Data Protection Principles
3. The Rights of Data Subjects
4. Lawful, Fair, and Transparent Data Processing
5. Specified, Explicit, and Legitimate Purposes
6. Adequate, Relevant, and Limited Data Processing
7. Accuracy of Data and Keeping Data Up-to-Date
8. Data Retention
9. Accountability and Record-Keeping
10. Data Protection Impact Assessments
11. Keeping Data Subjects Informed
12. Data Subject Access
13. Rectification of Personal Data
14. Erasure of Personal Data
15. Restriction of Personal Data Processing
16. Data Portability
17. Objections to Personal Data Processing
18. Automated Decision-Making
19. Profiling
20. Personal Data Collected, Held, and Processed
21. Data Security - Transferring Personal Data and Communications
22. Data Security - Storage
23. Data Security - Disposal
24. Data Security - Use of Personal and Sensitive Data
25. Data Security - IT Security
26. Organisational Measures
27. Department Responsibilities
28. Users’ Responsibilities
29. Transferring Personal Data to a Country Outside the EEA
30. Data Breach Notification
31. Policy Review
32. Implementation of Policy

Appendix 1 - List of locations

Appendix 2- Full list of Data held

Appendix 3 - Data Protection Impact Assessments

1. Introduction

This Policy sets out the obligations of the CCiW a charity registered in the UK under number 1079713 and a Limited Company under reg. No. 3900844, whose registered office is at **6 RESTORMEL ROAD, NEWLYN, PENZANCE, CORNWALL TR18 5QPL** (“the Charity”) regarding data protection and the rights of customers, contacts, employees and supporters (“data subjects”) in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation (“GDPR”).

The GDPR defines “personal data” as any information relating to an identified or identifiable natural person (a “data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

This Policy sets the CCiW’s obligations regarding the collection, processing, transfer, storage, retention and disposal of personal data. The procedures and principles set out herein must be followed at all times by the CCiW, its employees, agents, contractors, or other parties working on behalf of the CCiW.

The CCiW is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

For the purposes of this Policy, “data” shall refer to the following type(s) of data:

Personal data;

Sensitive data;

Financial data that could be linked to a person;

Confidential data.

1. The Data Protection Principles

This Policy aims to ensure compliance with the GDPR. The GDPR sets out the following principles with which any party handling personal data must comply. All 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. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
    3. Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
    4. Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, 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 is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject.
    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.

1. The Rights of Data Subjects

The GDPR sets out the following rights applicable to data subjects (please refer to the parts of this policy indicated for further details):

* + 1. The right to be informed (Part 12).
    2. The right of access (Part 13);
    3. The right to rectification (Part 14);
    4. The right to erasure (also known as the ‘right to be forgotten’) (Part 15);
    5. The right to restrict processing (Part 16);
    6. The right to data portability (Part 17);
    7. The right to object (Part 18); and
    8. Rights with respect to automated decision-making and profiling (Parts 19 and 20).

1. Lawful, Fair, and Transparent Data Processing
   * 1. The GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The GDPR states that processing of personal data shall be lawful if at least one of the following applies:
        + 1. The data subject has given consent to the processing of their personal data for one or more specific purposes;
          2. The processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them;
          3. The processing is necessary for compliance with a legal obligation to which the data controller is subject;
          4. The processing is necessary to protect the vital interests of the data subject or of another natural person;
          5. The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or
          6. The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
     2. If the personal data in question is “special category data” (also known as “sensitive personal data”) (for example, data concerning the data subject’s race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation), at least one of the following conditions must be met:
        + 1. The data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless EU or EU Member State law prohibits them from doing so);
          2. The processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by EU or EU Member State law or a collective agreement pursuant to EU Member State law which provides for appropriate safeguards for the fundamental rights and interests of the data subject);
          3. The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
          4. The data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects;
          5. The processing relates to personal data which is clearly made public by the data subject;
          6. The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;
          7. The processing is necessary for substantial public interest reasons, on the basis of EU or EU Member State law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;
          8. The processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of EU or EU Member State law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the GDPR;
          9. The processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of EU or EU Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or
          10. The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the GDPR based on EU or EU Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.
2. Specified, Explicit, and Legitimate Purposes
   * 1. The CCiW collects and processes the personal data set out in Part 21 of this Policy. This includes:
        + 1. Personal data collected directly from data subjects; and
          2. Personal data obtained from third parties.
     2. The CCiW only collects, processes, and holds personal data for the specific purposes set out in Part 21 of this Policy (or for other purposes expressly permitted by the GDPR).
     3. Data subjects are kept informed at all times of the purpose or purposes for which the CCiW uses their personal data. Please refer to Part 12 for more information on keeping data subjects informed.
     4. All data must be classified appropriately (including, but not limited to, personal data, sensitive personal data, and confidential information). All data so classified must be handled appropriately in accordance with its classification.
3. Adequate, Relevant, and Limited Data Processing

The CCiW will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Part 5, above, and as set out in Part 21, below.

1. Accuracy of Data and Keeping Data Up-to-Date
   * 1. The CCiW shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Part 14, below.
     2. The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.
2. Data Retention

8.1 The GDPR includes the right to erasure or “the right to be forgotten”. Data subjects have the right to have their personal data erased (and to prevent the processing of that personal data) in the following circumstances:

Where the personal data is no longer required for the purpose for which it was originally collected or processed (see above);

When the data subject withdraws their consent;

When the data subject objects to the processing of their personal data and the CCiW has no overriding legitimate interest;

When the personal data is processed unlawfully (i.e. in breach of the GDPR);

When the personal data has to be erased to comply with a legal obligation; or

Where the personal data is processed for the provision of information society services to a child.

* + 1. The CCiW shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.
    2. When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

8.4 This section sets out the type(s) of personal data held by the CCiW in various departments, the period(s) for which that personal data is to be retained, the criteria for establishing and reviewing such period(s), and when and how it is to be deleted or otherwise disposed of.

8.5 A list (appendix 1) will be kept of locations where data is stored by the CCiW. This will include CCiW hardware and devices, third-party servers, mobile devices, computers and devices owned by volunteers and/or contractors used in accordance with the WOYD policy and physical records.

I think this is meant to be WYOD Policy

WYOD – Wear Your Own Device

These are policies that cover the use of smart watches, etc.

CCiW does not have such a policy. I would suggest that we do not need a specific policy, but include these types of the list of devices references in this policy.

* + 1. Different types of personal data, used for different purposes, will necessarily be retained for different periods (and its retention periodically reviewed), as set out below.
    2. When establishing and/or reviewing retention periods, the following shall be taken into account:

The objectives and requirements of the CCiW;

The type of personal data in question;

The purpose(s) for which the data in question is collected, held, and processed;

The CCiW’s legal basis for collecting, holding, and processing that data;

The category or categories of data subject to whom the data relates;

* + 1. If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can be regularly reviewed against those criteria.
    2. Notwithstanding the following defined retention periods, certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made within the CCiW to do so (whether in response to a request by a data subject or otherwise).
    3. In limited circumstances, it may also be necessary to retain personal data for longer periods where such retention is for archiving purposes that are in the public interest, for historical research purposes, or for statistical purposes. All such retention will be subject to the implementation of appropriate technical and organisational measures to protect the rights and freedoms of data subjects, as required by the GDPR.
    4. This policy includes a list of the type of data used by the CCiW including retention periods (section 21);

1. Secure Processing

The CCiW shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided in Parts 21 to 29 of this Policy.

1. Accountability and Record-Keeping
   * 1. The Trustees of the CCiW shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the CCiW’s other data protection-related policies, and with the GDPR and other applicable data protection legislation.
     2. The CCiW shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information (Appendix 2):
        + 1. The purposes for which the CCiW collects, holds, and processes personal data;
          2. Details of the categories of personal data collected, held, and processed by the CCiW, and the categories of data subject to which that personal data relates;
          3. Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;
          4. Details of how long personal data will be retained by the CCiW; and
          5. Descriptions of all technical and organisational measures taken by the CCiW to ensure the security of personal data.
2. Data Protection Impact Assessments
   * 1. The CCiW shall carry out Data Protection Impact Assessments for any new project that uses personal data in a way not done before.
     2. Data Protection Impact Assessments shall be overseen by the Office managers:

As far as I am aware, we do not have ‘Office Managers’. They are referred to frequently in this policy.

I think in this section, the responsibility should be with trustees.

* + - * 1. The type(s) of personal data that will be collected, held, and processed;
        2. The purpose(s) for which personal data is to be used;
        3. The CCiW’s objectives;
        4. How personal data is to be used;
        5. The parties (internal and/or external) who are to be consulted;
        6. The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
        7. Risks posed to data subjects;
        8. Risks posed both within and to the CCiW; and
        9. Proposed measures to minimise and handle identified risks.
    1. Details of DPIA can be found in Appendix 3

1. Keeping Data Subjects Informed
   * 1. The CCiW shall provide the information set out in Part 12.2 to every data subject:
        + 1. Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and
          2. Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:

as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

* + 1. The following information shall be provided:
       - 1. Details of the CCiW;
         2. The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 21 of this Policy) and the legal basis justifying that collection and processing;
         3. Where applicable, the legitimate interests upon which the CCiW is justifying its collection and processing of the personal data;
         4. Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;
         5. Where the personal data is to be transferred to one or more third parties, details of those parties;
         6. Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the “EEA”), details of that transfer, including but not limited to the safeguards in place (see Part 30 of this Policy for further details);
         7. Details of data retention;
         8. Details of the data subject’s rights under the GDPR;
         9. Details of the data subject’s right to withdraw their consent to the CCiW’s processing of their personal data at any time;
         10. Details of the data subject’s right to complain to the Information Commissioner’s Office (the “supervisory authority” under the GDPR);
         11. Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and
         12. Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

1. Data Subject Access
   * 1. Data subjects may make subject access requests (“SARs”) at any time to find out more about the personal data which the CCiW holds about them, what it is doing with that personal data, and why.
     2. Employees wishing to make a SAR should do so via the Office managers of the CCiW.

As far as I am aware, we do not have ‘Office Managers’. They are referred to frequently in this policy.

I think in this section, the responsibility should be with trustees.

I am not aware of any employees.

We should probably have something glike;

Camp Leaders make a SAR via trustees.

Other volunteers involved with a camp make a SAR via their camp leader.

Volunteers not involved with a camp, make a SAR via trustees.

It might be worth keeping the employee reference in case CCiW has any employees in the future.

* + 1. Responses to SARs shall normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.
    2. The CCiW does not charge a fee for the handling of normal SARs. The CCiW reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

1. Rectification of Personal Data
   * 1. Data subjects have the right to require the CCiW to rectify any of their personal data that is inaccurate or incomplete.
     2. The CCiW shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the CCiW of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.
     3. In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.
2. Erasure of Personal Data
   * 1. Data subjects have the right to request that the CCiW erases the personal data it holds about them in the following circumstances:
        + 1. It is no longer necessary for the CCiW to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;
          2. The data subject wishes to withdraw their consent to the CCiW holding and processing their personal data;
          3. The data subject objects to the CCiW holding and processing their personal data (and there is no overriding legitimate interest to allow the CCiW to continue doing so) (see Part 18 of this Policy for further details concerning the right to object);
          4. The personal data has been processed unlawfully;
          5. The personal data needs to be erased in order for the CCiW to comply with a particular legal obligation.
     2. Unless the CCiW has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject’s request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.
     3. In the event that any personal data that is to be erased in response to a data subject’s request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).
3. Restriction of Personal Data Processing
   * 1. Data subjects may request that the CCiW ceases processing the personal data it holds about them. If a data subject makes such a request, the CCiW shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.
     2. In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).
4. Data Portability
   * 1. The CCiW processes personal data using automated means through our online form management system.
     2. Where data subjects have given their consent to the CCiW to process their personal data in such a manner, or the processing is otherwise required for the performance of a contract between the CCiW and the data subject, data subjects have the right, under the GDPR, to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers).
     3. To facilitate the right of data portability, the CCiW shall make available all applicable personal data to data subjects in PDF format.
     4. All requests for copies of personal data shall be complied with within one month of the data subject’s request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed.
5. Objections to Personal Data Processing
   * 1. Data subjects have the right to object to the CCiW processing their personal data based on legitimate interests, direct marketing (including profiling), and processing for historical research and statistics purposes.
     2. Where a data subject objects to the CCiW processing their personal data based on its legitimate interests, the CCiW shall cease such processing immediately, unless it can be demonstrated that the CCiW’s legitimate grounds for such processing override the data subject’s interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.
     3. Where a data subject objects to the CCiW processing their personal data for direct marketing purposes, the CCiW shall cease such processing immediately.
     4. Where a data subject objects to the CCiW processing their personal data for historical research and statistics purposes, the data subject must, under the GDPR, “demonstrate grounds relating to his or her particular situation”. The CCiW is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.
6. Automated Decision-Making
   * 1. The CCiW uses personal data in automated decision-making processes such as allocation of accommodation and tickets for events.
     2. Where such decisions have a legal (or similarly significant effect) on data subjects, those data subjects have the right to challenge to such decisions under the GDPR, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from the CCiW.
     3. The right described in Part 19.2 does not apply in the following circumstances:
        + 1. The decision is necessary for the entry into, or performance of, a contract between the CCiW and the data subject;
          2. The decision is authorised by law; or
          3. The data subject has given their explicit consent.
7. Profiling
   * 1. The CCiW does not currently use personal data for profiling purposes.
8. Personal Data Collected, Held, Processed and Retention Period

The following personal data is collected, held, and processed by the CCiW:

| **Data Ref.** | **Type of Data** | **Purpose of Data** | **Review Period** | **Retention Period or Criteria** | **Comments** |
| --- | --- | --- | --- | --- | --- |
| CCiWD101 | Personal sensitive data (name, address, phone number, email, language preference, DBS status, church) | To be used for genuine operational uses within the organisation e.g. contacting committee members. | Annually | Not fixed | Such data is held by the CCiW so that we can contact people or groups regularly for operational needs. |
| CCiWD102 | Personal sensitive data (name, address, phone number, email, language preference, church) | To be used before and during an event or ministry for a specific contractual reason e.g. booking for a camp. | No review | 12 months |  |
| CCiWD103 | Personal sensitive data (name, address, phone number, language preference, church) | If client has opted in to receive marketing material within a specific ministry e.g. posting camp flyer. | Annually | 3 years from last contact |  |
| CCiWD104 | Personal sensitive data from donors (name, address, phone number, email, language preference, gift aid, church) | To contact with news and fundraising. | Annually | 5 years |  |
| CCiWD105 | Personal (name, email, language preference) | If customer has opted in then emails sent for marketing and information purposes e.g. prayer letter or leaders information. | 6 months | 12 months from inactivity | Campaign monitor allows for unsubscribing |
| CCiWD106 | Sensitive U18 (medical, behavioural, DOB) | To keep children safe during events e.g. Parental consent form for camps. | No review | 12 weeks after event |  |
| CCiWD107 | Personal sensitive data (religious, DOB, medical, and references, DBS status) | To ensure that all staff, volunteers and other contacts are correctly vetted in line with our policies e.g. camp officers. | Annually | 3 years from last reference |  |
| CCiWD108 | Financial information – general (Name, address, email, amount and method of payment) | Record keeping and accounting e.g. camp booking. | Annually | 7 years |  |
| CCiWD109 | Financial information – sensitive (Name, address, email, card number and details) | To take payments for one off events and resources e.g. postal camp booking form. | No review | 0 days |  |
| CCiWD110 | Financial information -sensitive | To take payments for recurring events and resources e.g. magazine subscriptions. | 6 months | 0 days from termination of payment | IS THIS NEEDED? |
| CCiWD111 | Personal sensitive data for staff and volunteers (religious, medical, DBS and references) | To ensure safety of staff e.g. staff contact forms. | Annually | 1 year from termination of contract |  |
| CCiWD112 | Social Media (name, interaction level) | As we use social media for marketing, we’re able to see who interacts with us e.g. Facebook event. | Annually | User can unsubscribe | We do not keep records outside of social media. |
| CCiWD113 | Sensitive data concerning religious activity | As part of our constitutional structures and genuine operational processes, data such as religious activity, comments will be stored within committee minutes. | Annually | Not fixed |  |
| CCiWD114 | Technical data  (Name, IP address, browser used, location of IP address) | To ensure booking forms and website perform efficiently e.g. Formstack and campaign monitor. | Annually | 12 weeks after event or 12 months after purchase | Replace these with the names of the software we use. |
| CCiWD115 | Church link representative data (Name, address, phone, email, church) | If they have consented to being a church representative then we keep details so that we can send general, marketing and fundraising information to them e.g. conference brochure. |  |  | Does CCiW have ‘Church link representatives? If not, remove this row. |

1. Data Security - Transferring Personal Data and Communications

The CCiW shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

* + 1. All emails containing personal and/or sensitive data must be sent from an CCiW authorised account;

I am not aware of any CCiW email accounts.

CCiW obviously has a domain name: [www.cciw.co.uk](http://www.cciw.co.uk)

Therefore, it would be possible to have cciw email accounts.

I would strongly recommend that this is done.

CCiW might qualify for a free Google account of Microsoft 365 account as a registered charity.

Accounts are then created for trustees, key volunteers and camp leaders.

If we decide others need to use email, we could set up shared email accounts.

* + 1. All sensitive information will only be sent with the consent of the office manager and:

As far as I am aware, we do not have ‘Office Managers’. They are referred to frequently in this policy.

I think in this section, the responsibility should be with trustees and/or Camp Leaders.

* + - 1. The CCiW will make every effort to minimise the amount of sensitive data it sends by email, using paper copies, encrypted devices and internal systems whenever possible;
      2. All emails containing sensitive personal data must be marked “confidential”;
    1. Sensitive personal data must be downloaded and transmitted over secure networks whenever possible; transmission over unsecured networks should only be used when no secure network is available;
    2. Personal and sensitive data contained in an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted;
    3. Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;
    4. Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using royal mail signed for delivery service; and
    5. All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked “confidential”.

1. Data Security - Storage

The CCiW shall ensure that the following measures are taken with respect to the storage of personal data:

* + 1. All employees and volunteers of the CCiW and all third parties authorised to use the IT Systems and data collected, held, and processed by the CCiW including, but not limited to, contractors and sub-contractors (collectively, “Users”), must ensure that they are familiar with this Policy and must adhere to and comply with it at all times.
    2. All line managers must ensure that all Users under their control and direction must adhere to and comply with this Policy at all times as required under paragraph 2.4.

As far as I am aware, we do not have ‘Office Managers’. They are referred to frequently in this policy.

I think in this section, the responsibility should be with trustees and/or Camp Leaders.

* + 1. All electronic copies of personal data should be stored securely using machines that require a password and have been protected against unauthorised access;
    2. All electronic copies of sensitive personal data should be stored securely on password protected CCiW machines or storage devices, unless written permission has been given by an Office manager (see WOYD policy);

As far as I am aware, we do not have ‘Office Managers’. They are referred to frequently in this policy.

I think in this section, the responsibility should be with trustees.

I think this is meant to be WYOD Policy

WYOD – Wear Your Own Device

These are policies that cover the use of smart watches, etc.

CCiW does not have such a policy. I would suggest that we do not need a specific policy, but include these types of the list of devices references in this policy.

* + 1. All hardcopies of personal and sensitive data should be stored securely in a locked box, drawer, cabinet, or similar;
    2. All electronic copies stored on physical, removable media should be stored securely on an CCiW USB storage device or similar;
    3. All personal data stored electronically on CCiW devices and in CCiW systems should be backed up weekly with backups stored offsite;
    4. No personal data should be stored on any device (including, but not limited to, laptops, tablets, and smartphones), that does not belong to the CCiW without the formal written approval of Office Manager, and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary; and

As far as I am aware, we do not have ‘Office Managers’. They are referred to frequently in this policy.

I think in this section, the responsibility should be with trustees and/or Camp Leaders.

* + 1. Personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the CCiW where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the GDPR (which may include demonstrating to the CCIW that all suitable technical and organisational measures have been taken – a booklet will be given to all volunteers).

We should require all volunteers working on camps to sign saying they agree to comply fully with this policy.

There are a number of issues with Section 23

Does CCiW have any IT Systems?

Does CCiW provide computers or storage devices?

Is there a secure place for storing hardcopies?

Is there currently any offsite backup system?

Recommendations:

1. Sign up for a Google account or Microsot 365 account (assume a free charity account is available). Both of these systems provide email services using the cciw.co.uk domain and provide file sharing facilities which would also act as an offsite back up. This would also allow management of accounts and give the ability to reset passwords, etc (see section 26).
2. Camp Leaders are either provided with a CCiW laptop or a CCiW storage device (large capacity USB stick of external hard drive). Whichever is provided, is set up by CCiW with suitable security software and remains the property of CCiW. We can then enforce that no volunteers have data on their personal devices.
3. Camp Leaders are provided with a lockable portable file box to store hardcopies of data at home and on camp. We also request that they keep them in a secure place.
4. Data Security - Disposal

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of.

1. Data Security - Use of Personal and Sensitive Data

The CCiW shall ensure that the following measures are taken with respect to the use of personal data:

* + 1. No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the CCiW requires access to any personal data that they do not already have access to, such access should be formally requested from the Office manager;

As far as I am aware, we do not have ‘Office Managers’. They are referred to frequently in this policy.

I think in this section, the responsibility should be with trustees and/or Camp Leaders.

* + 1. No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the CCIW or not, without the authorisation of the Office manager;

As far as I am aware, we do not have ‘Office Managers’. They are referred to frequently in this policy.

I think in this section, the responsibility should be with trustees and/or Camp Leaders.

* + 1. Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time;
    2. If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it; and
    3. Where personal data held by the CCiW is used for marketing purposes, it shall be the responsibility of Office managers to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

As far as I am aware, we do not have ‘Office Managers’. They are referred to frequently in this policy.

I think in this section, the responsibility should be with trustees.

1. Data Security - IT Security

The CCiW shall ensure that the following measures are taken with respect to IT and information security:

* + 1. All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters and numbers or symbols;
    2. Passwords should not be written down or shared between any employees, agents, contractors, or other parties working on behalf of the CCiW, irrespective of seniority or department (apart from storing in a locked secure cabinet or safe). If a password is forgotten, it must be reset using the applicable method;
    3. All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. The CCiW shall be responsible for installing all security-related updates as soon as reasonably and practically possible, unless there are valid technical reasons not to do so;
    4. No software may be installed on any CCiW-owned computer or device without the prior approval of the Office managers;

As far as I am aware, we do not have ‘Office Managers’. They are referred to frequently in this policy.

I think in this section, the responsibility should be with trustees.

* + 1. The CCiW will keep a central list of all CCiW hardware and devices that holds sensitive and/or personal information;
    2. Any non-CCiW machine used to deal with CCiW personal data must have a full and valid security system and password protection.

How would this be enforced and monitored?

1. Organisational Measures

The CCiW shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

* + 1. Handbooks will be produced giving clear and practical guidelines to the following groups:
       - 1. Trustees
         2. Administrative Volunteers
         3. Camp Leaders
         4. Camp Officers
    2. All employees, volunteers, agents, contractors, or other parties working on behalf of the CCiW shall be made fully aware of both their individual responsibilities and the CCiW’s responsibilities under the GDPR and under this Policy, and shall be provided with a copy of this Policy;
    3. Only employees, volunteers, agents, sub-contractors, or other parties working on behalf of the CCiW that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the CCiW;
    4. All employees, volunteers, agents, contractors, or other parties working on behalf of the CCiW handling personal data will be appropriately trained to do so;

This would be a good thing and considered Best Practice. However, can we realistically commit to doing this for ALL volunteers?

* + 1. All employees, volunteers, agents, contractors, or other parties working on behalf of the CCiW handling personal data will be appropriately supervised;

Supervised by who?

* + 1. All employees, volunteers, agents, contractors, or other parties working on behalf of the CCiW handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;
    2. Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;
    3. All personal data held by the CCIW shall be reviewed periodically, as set out in the CCiW’s Data Retention Policy;
    4. The performance of those employees, volunteers, agents, contractors, or other parties working on behalf of the CCiW handling personal data shall be regularly evaluated and reviewed;
    5. All employees, volunteers, agents, contractors, or other parties working on behalf of the CCiW handling personal data will be bound to do so in accordance with the principles of the GDPR and this Policy by contract;
    6. All agents, volunteers, contractors, or other parties working on behalf of the CCiW handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the CCiW arising out of this Policy and the GDPR; and
    7. Where any agent, volunteers, contractor or other party working on behalf of the CCiW handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the CCIW against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

1. Department Responsibilities
   * 1. The Office Managers, shall be responsible for the following:

As far as I am aware, we do not have ‘Office Managers’. They are referred to frequently in this policy.

I think in this section, the responsibility should be with trustees and/or Camp Leaders.

This section also refers to Senior Management. This should be trustees.

The board may need to appoint;

Data Protection Officer – responsible for many items listed in this policy for Office Manager.

[We could have a compliance officer to oversee this and other policies]

IT Officer – responsible for the IT related elements of this policy and other IT related issues.

ensuring that all IT Systems are assessed and deemed suitable for compliance with the CCiW’s security requirements;

ensuring that IT security standards within the CCiW are effectively implemented and regularly reviewed, working in consultation with the CCiW’s senior management and reporting the outcome of such reviews to the CCiW’s senior management;

ensuring that all Users are kept aware of the IT-related requirements of this Policy and of all related legislation, regulations, and other relevant rules whether now or in the future in force including, but not limited to, the GDPR and the Computer Misuse Act 1990.

ensuring that all other data processing systems and methods are assessed and deemed suitable for compliance with the CCiW’s security requirements;

ensuring that data security standards within the CCiW are effectively implemented and regularly reviewed, working in consultation with the CCiW’s senior management and Office managers, as appropriate, and reporting the outcome of such reviews to the CCiW’s senior management;

ensuring that all Users are kept aware of the non-IT-related requirements of this Policy and of all related legislation, regulations, and other relevant rules whether now or in the future in force including, but not limited to, the GDPR.

assisting all Users in understanding and complying with the IT-related aspects of this Policy;

providing all Users with appropriate support and training in IT security matters and use of IT Systems;

ensuring that all Users are granted levels of access to IT Systems that are appropriate for each User, taking into account their job role, responsibilities, and any special security requirements;

receiving and handling all reports relating to IT security matters and taking appropriate action in response;

taking proactive action, where possible, to establish and implement IT security procedures and raise User awareness;

Reviewing non-CCiW devices in line with the WOYD policy;

assisting the IT Manager in monitoring all IT security within the CCiW and taking all necessary action to implement this Policy and any changes made to this Policy in the future;

ensuring that regular backups are taken of all data stored within the IT Systems at intervals no less than one week and that such backups are stored at a suitable location offsite.

assisting all Users in understanding and complying with the non-IT-related aspects of this Policy;

providing all Users with appropriate support and training in data security matters;

ensuring that all Users are granted levels of access to data that are appropriate for each User, taking into account their job role, responsibilities, and any special security requirements;

receiving and handling reports concerning non-IT-related data security matters and taking appropriate action in response: and

taking proactive action, where possible, to establish and implement security procedures and raise User awareness.

1. Users’ Responsibilities
   * 1. All Users must comply with all relevant parts of this Policy and the WOYD Policy at all times when using the IT Systems and data.
     2. All Users must use the IT Systems and data only within the bounds of UK law and must not use the IT Systems or data for any purpose or activity which is likely to contravene any UK law whether now or in the future in force.
     3. Users must immediately inform the Office managers of any and all security concerns relating to the IT Systems or data.
     4. Users must immediately inform the Office managers of any other technical problems (including, but not limited to, hardware failures and software errors) which may occur on the IT Systems.
     5. Any and all deliberate or negligent breaches of this Policy by Users will be handled as appropriate under the CCiW’s disciplinary procedures.
2. Transferring Personal Data to a Country Outside the EEA
   * 1. The CCiW may from time to time transfer (‘transfer’ includes making available remotely) personal data to countries outside of the EEA.
     2. The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:
        + 1. The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data;
          2. The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner’s Office); certification under an approved certification mechanism (as provided for in the GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;
          3. The transfer is made with the informed consent of the relevant data subject(s);
          4. The transfer is necessary for the performance of a contract between the data subject and the CCIW (or for pre-contractual steps taken at the request of the data subject);
          5. The transfer is necessary for important public interest reasons;
          6. The transfer is necessary for the conduct of legal claims;
          7. The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or
          8. The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.
3. Data Breach Notification
   * 1. All personal data breaches must be reported immediately to the Office managers of the CCIW.
     2. If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer (DPO) must ensure that the Information Commissioner’s Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.
     3. In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 29.2) to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

A DPO is not a legal requirement, but it is recommended.

* + 1. Data breach notifications shall include the following information:
       - 1. The categories and approximate number of data subjects concerned;
         2. The categories and approximate number of personal data records concerned;
         3. The name and contact details of the CCiW office manager (or other contact point where more information can be obtained);
         4. The likely consequences of the breach;
         5. Details of the measures taken, or proposed to be taken, by the CCiW to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

1. Policy Review

The CCiW shall review this Policy not less than 3 years and otherwise as required in order to ensure that it remains up-to-date and fit for purpose. All questions, concerns, and other feedback relating to this Policy should be communicated to the CCiW trustee for services, as appropriate.

1. Implementation of Policy

This Policy shall be deemed effective as of 25/5/2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

**Name: Position:**

**Date: Review Date:**

**Signature**

**Appendix 1**

**List of locations**

|  |  |  |  |
| --- | --- | --- | --- |
| Location | Category of Data | Specific security instructions | Responsibility |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

We will need to audit the trust to complete this report.

Once complete we may need to consolidate storage of data to make it easier to comply with this policy.

**Appendix 2**

**Full list of Data held**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Category of Data | Type of Data | Location | Retention Period | Linked data | Responsibility |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

We will need to audit the trust to complete this report.

Once complete we may need to consolidate recording of data to make it easier to comply with this policy.

**Appendix 3**

**Data Protection Impact Assessments**

Data Protection is primarily concerned with preventing harm or distress to individuals when you use their data. The notion of harm can be somewhat abstract, and so this guide is intended to help you:

* identify data risks
* assess their likelihood and severity
* determine appropriate measures to reduce or eliminate the risk

**How do I identify a risk?**

List every place in which your data is collected, stored, and used. Consider each in turn, and identify ways in which the data could be compromised – this does not just mean stolen; it can also mean damaged, corrupted, lost, or disclosed. These are your data risks.

**How do I assess a risk?**

There are two measures you should be concerned with when assessing the severity of a risk – how likely it is to happen, and the severity of the consequences where it does happen.

|  |  |
| --- | --- |
| **Likelihood (Score)** | **Description** |
| 1 | Measures are in place, so the situation is not likely to occur. Have no knowledge of this happening. The situation has never occurred in the CCiW and may only occur under very exceptional circumstances. |
| 2 | Measures are in place, but the situation could occur once in the next 30 years. |
| 3 | Measures are in place, but the situation could occur anytime in the next 5 years. |
| 4 | The situation has occurred elsewhere in the CCiW under similar circumstances with similar control measures. Some history of near miss incidents. This situation occurs at least once per year in our ministry, and is likely to occur again in the next year. Initial events have occurred, but the negative consequences did not materialise because of chance, not because of planned/existing control measures. There is a history of near miss incidents. |
| 5 | This situation exists now. There are common repeating occurrences. The situation will occur again very soon. Consequences are expected to occur in most circumstances. |

|  |  |
| --- | --- |
| **Severity (Score)** | **Description** |
| 1 | No harm will be caused to data subjects. No damage to CCiW’s reputation. Loss or damage of data will not cause financial or reputational harm to CCiW as a gospel organisation. |
| 2 | This will cause minimal harm or distress to the data subjects. Unlikely to damage CCiW’s reputation. Loss or damage of data is unlikely cause financial or reputational harm to CCiW as a gospel organisation. |
| 3 | Data subjects may be inconvenienced or experience minor emotional or mental distress. CCiW may suffer reputational and relational damage. Loss or damage of data may cause financial or reputational harm to CCiW as a gospel organisation. |
| 4 | Data subjects will be inconvenienced. Data subjects may experience unacceptable emotional or mental distress, or physical discomfort. Data subjects may experience minor financial loss. CCiW are likely to suffer reputational damage. Loss or damage of data likely to cause financial or reputational harm to CCiW as a gospel organisation. |
| 5 | This will cause physical injury, emotional or mental damage, or financial harm to the data subjects. CCiW will suffer major reputational damage. CCiW could face legal action. Loss or damage of data will cause financial or reputational harm to CCiW as a gospel organisation. |

For the severity or likelihood category to apply, only one criteria in that category needs to be true, and you always choose the highest that applies. For example, if a risk would cause no harm to CCiW’s reputation (level 1) but would cause minor financial loss to data subjects (level 4) you would select level 4 as the appropriate level of severity. You then assign a score by multiply the two values together. This gives you the risk score. You should now have a risk assessment table, like the example below:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Data Project: | Camp medical information |  |  |  |
| Risk | Likelihood | Severity | Score | Action |
| Data may be accessed off CCiW machine | 1 | 5 | 5 | Follow CCiW protocols |
| Data may go missing in the post | 1 | 5 | 5 | Follow CCiW protocols |
| Officer may leave data where others can see | 4 | 5 | 20 | Provide special folder for medical officer. |
| Officer may lose data on trip or during a camp | 2 | 5 | 10 | Follow CCiW protocols, but remember to log data back when received |

**Risk Matrix:**

|  |  |  |
| --- | --- | --- |
| Risk Level | Risk Description | Action |
| 16 to 25 | Very High | These risks are unacceptable. Senior management attention is needed. Risk treatment action plans are required. Substantial improvements in risk control are very necessary to ensure that the risk is reduced, within a defined time frame. The work activity shall be halted until risk control measures are implemented that reduces the risk so that it is no longer very high. If it is not possible to reduce the risk, then the work shall remain prohibited. |
| 10 to 15 | High | Substantial effort shall be made to reduce the risk. Risk treatments shall be identified and implemented urgently within a defined period, and it may be necessary to consider suspending or restricting the activity, or to apply interim control measures. Considerable resources might have to be allocated to additional risk treatments. Arrangements shall be made to ensure that risk control measures are maintained. |
| 5 to 9 | Moderate Risks | Risks are to be addressed in order of priority, leading to continuous improvement. Once actions are planned, they shall be implemented within a defined period of time, tracked to completion, and arrangements shall be made to ensure that risk control measures are maintained. |
| 1 to 4 | Low | These risks are considered low. No additional risk treatments are required unless they can be implemented with minimal resources. |

**What action do I need to take?**

You should rank the risks in order from highest to lowest, and address your highest risks first. In the first instance, you must identify if it is possible to take any measure to address this risk. If no measures are possible, and the risk is High or Very High you must not use the data.

Where measures have been identified, you are required to note them in your assessment, and then to assign a person to be responsible for implementing these measures. In all instances, you may seek the advice of the Data Protection Officer.