**A picture containing object

Description generated with very high confidence**

**EMW Data Protection Handbook**

**Office Staff**

**2018-2019**

**Draft Copy**

**Contents**

3 ………… Introduction

4 ………… What is the GDPR?

5 ………… What is personal data

6 ………… Should I collect and use personal data?

7 ………… Guidelines for collecting personal data and ongoing processes

9 ………… Guidelines for storing personal data

10 …….… Guidelines on keeping data up to date and responding to requests.

11 ………. Guidelines on transferring personal data

13 ………. Guidelines for using personal data

14 ………. Guidelines for disposing of data

15 ………. Recording a breach

16 ………. Worked examples and checklist

17 ………. List of important documents

18 ………. Contact details

**Introduction**

Data Protection law changed in the UK on 25 May 2018.

The law will impact how we handle personal data in our work. CCiW has adopted a new ‘Data Protection, Security and Retention Policy’ and a ‘Working on your own device policy’ (WOYD), and all trustees, leaders and admin volunteers are required to have read the policies and to be familiar with the good data protection practice specified in the policies.

This handbook will give you a simple and brief introduction on how to recognise personal data and know how to use it in line with our policy. In simple terms we want to leaders and admin volunteers to comply with the GDPR and be comfortable with the changes to the law.

Leaders and admin volunteers are especially required to be aware of their role in helping trustees to be compliant with data protection law; all volunteers represent EMW when they hold personal data, and any breach of data protection law by a volunteer impacts us all, not just the individual. We therefore need to advise you that failure to comply may result in the staff disciplinary procedure being initiated.

If you are unsure about any aspect of the regulation, policy and/or your own responsibilities, there is an open-door policy to any member of the trustees.

As the EMW is such a wide-ranging organisation that involves staff, volunteers and others we’ve decided on a three-level system to ensure that we are compliant. These are:

1. Website master, booking officer, finance officer,

DBS officer Camp Leaders Main responsibility

1. Volunteers Least responsibility

**Key Concept!**

***You’re not alone, but you must ask for help.***

**What is the GDPR?**

The GDPR sets out the following principles with which any organisation handling personal data must comply. All personal data must be:

* Processed lawfully, fairly, and in a transparent manner in relation to the data subject.
* 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.
* Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
* 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.
* 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 to safeguard the rights and freedoms of the data subject.
* 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.

**Key Concept!**

***We must deal with people’s data with respect.***

**What is personal data?**

Personal data is, in simpler terms, any information about a person that enables them to be identified. Personal data covers obvious information such as name and contact details, but it also covers less obvious information such as identification numbers, electronic location data, and other online identifiers.

This means some types of information should *always* be considered as personal data:

* Any information that enables a person to be contacted (this includes postal address, email address, telephone numbers, or any other means)
* Financial information such as bank details, salary, or expenditure

You are required to take specific care with special category data. This is data specified in the GDPR as being more sensitive, and so needs more protection. For example, information about an individual’s:

* Race;
* Ethnic origin;
* Politics;
* Religion;
* Trade union membership;
* Genetics;
* Biometrics (where used for ID purposes);
* Health;
* Sexual orientation.

These must always be considered personal data, and must always satisfy additional safety requirements, which are set out in the Data Protection Policy.

Given that CCiW is a faith-based charity, you will inevitably handle personal data relating to the religion of others, such as church attendance or theological beliefs. CCiW has a legitimate interest as a faith charity to process this data, and a legal justification to process the sensitive data provided it is for the purposes of the charity’s objectives.

Some information is regarded as personal data by the act, but may be appropriate for you to collect

given the relational nature of our ministries. Examples include:

* Marital status
* Names and ages of children
* Birthday
* Opinions about others (for example – collecting references for a specific role)

A flowchart is available from the Information Commissioner’s Website to help you determine whether the data you are considering is personal data:

<https://ico.org.uk/media/fororganisations/documents/1549/determining_what_is_personal_data_quick_reference_guide.pdf>

**Key Concept!**

***If it identifies a person, it’s personal and you need to take care.***

**Should I collect and use personal data?**

As an organisation we should only collect and use personal data that we need to carry out our work and ministry. The question to ask is – do I need this information?

You should avoid personal data where the following may apply:

* Using the data could cause harm to an individual.
* Using the data could cause embarrassment or distress to an individual.
* Using the data could enable others to contact the individual without permission to do so.
* Using the data may not reflect the wishes of the individual.

Examples

* I do need to know if a child has behavioural problems if he’s coming on camp, because the leaders and officers need to be able to look after the child correctly.
* I don’t need to know if a child is on Facebook as we don’t use Facebook as a primary means of communication with children.
* I do need the address of a person who orders a magazine.

As a leader, you’re expected to identify possible issues with our volunteers when collecting data – if in doubt just ask.

During September/October every year we will review our procedures to make sure that application, booking and order forms are correct.

**Key Concept!**

***If you don’t need it, don’t ask for it.***

**Guidelines for collecting personal data and ongoing processes.**

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).

This means that when you are collecting information on somebody you must tell them:

* What information you are collecting;
* Why you are collecting the information;
* How it will be stored;
* How somebody can erase or edit their information.

Additionally, where you are looking to communicate by email, the law on electronic communication requires you to have the consent of the individual.

Given the nature of CCiW, you will most likely receive information through booking forms etc that include a ‘consent’ box. This will give clear instructions how you can use the information. **You should never fill a form on behalf of somebody else or produce a form that has an automatic ‘opt-in’ consent box.**

Training will be given to show how to word any sentence linked to an opt-in box on a form.

Given the relational nature of CCiW, it is likely that some exchanges of personal data will be verbal, or will involve someone sending you a text, email, or social media message with their contact information.

When you receive personal data from an individual, you should make clear that you are receiving the data on behalf of CCiW, and not as an individual. This means that you are then able to share this data with other CCiW volunteers, because the data has been given to CCiW and not to you.

If you are given verbal consent to contact someone (e.g. somebody calls or sends a letter), please send the following communication (details amended as appropriate):

*I am confirming that I received your email address [email@emailhost.com] when I spoke with you at [place] on [date], and you gave the CCiW permission to contact you at this email regarding CCiW events and activities. If you change your mind, you can withdraw your consent at any stage by replying to this email address [cciw@] or by telephoning [0XXXX XXX XXX].*

(NB – if you received a telephone number or postal address, the same text applies, except you replace the email address with the appropriate communication. You may include as many means of communication as were given by the individual)

If an individual sends you an email with their details, please send the following acknowledgement:

*Thank you for your email below. This reply confirms that I have received it, and that you have given your consent for CCiW to contact you using the contact information provided in it, including the email address. . If you change your mind, you can withdraw your consent at any stage by replying to this email address [cciw@] or by telephoning [0XXXX XXX XXX].*

In both cases, send a copy of the email to yourself, and save a PDF copy of the email to the archive in a folder specifically for recording consent.

The file name should be as follows:

YEAR | MONTH | DATE | SURNAME | FIRSTNAME – Consent

For example – 20181031 Bloggs Joe – Consent means you emailed Joe Bloggs on 31 October 2018 to record their consent.

**You must then add their details to the appropriate mailing/emailing list.**

This means that if challenged, we have a record of the consent saved somewhere that can be easily

found, and you prove:

* You were given verbal permission to use their details;
* You communicated how you planned to use the data;
* You gave them the chance to withdraw their consent at the time, and in future.

Leaders and admin volunteers are required to consider data protection ‘by design and default’; meaning that you should be actively looking out where you are using personal data in your work, and ensuring that any use is compliant with the GDPR. As part of this, you may have to undertake a Data Protection Impact Assessment (DPIA) for any new project that uses personal data.

If you think you might need to conduct a DPIA you should contact a trustee, who will guide you through the process of completing the assessment, and sign off on the new use of personal data. You do not need to conduct a DPIA for any project that has already been approved by CCiW previously, unless the nature of the project has substantively changed.

**Key Concept!**

***If you’ve got it, then you collected it, and you therefore should have told them!***

**Guidelines for storing personal data.**

Personal and sensitive data is valuable, and you should therefore store it carefully.

Please remember the following important principles:

* Only use EMW computers, programmes and systems to store personal and sensitive information.
* If you are using your own machine (e.g. phone) to store or access information, then you must have written permission from your line manager to do so.
* Any personal or sensitive information you store or access on paper must be stored in a locked cabinet or safe.

You are required by law, and by CCiW’s Data Protection Policy, to ensure the security and integrity of the data you hold. This means:

* Preventing unauthorised access to the data.
* Preventing public disclosure of the data.
* Preventing the loss of the data.
* Preventing unauthorised use of the data.
* Preventing the corruption or destruction of the data.

**A word on security**

It is your responsibility to keep your working environment safe. This includes:

* Make sure that any passwords you have written down are locked in a cabinet/safe.
* Do not store any password on your machines.
* Make sure that you set your computer to automatically lock down after 30 mins of inactivity.
* Never leave personal sensitive information where somebody else could see it.
* Make sure your computer has up-to date virus software.
* Do not download software on to your computer without the written agreement of your line manager.

**A word on retention**

We are only allowed to store information on people for as long as it is needed. Details of this can be found in section 8 of the policy. Never keep data for longer than is necessary.

**Key Concept!**

**Guidelines on keeping data up to date and responding to requests.**

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.

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.

As a CCiW admin worker or leader it is your responsibility to keep records up to date and accurate. This means that you must:

* Update systems if there are changes in contact details;
* Check contact details after an event;
* Check permissions (opt-in and opt-out) after every event.
* Remove information from the system when it needs to be erased.

**A word on SARs**

People may make subject access requests (“SARs”) at any time to find out more about the personal data which the EMW holds about them, what it is doing with that personal data, and why.

If you receive a SAR, please pass on to one of the office managers within 1 day or receiving such a request.

**Key Concept!**

***The less information we keep on people, the easier it will be to keep information up-to-date.***

**Guidelines on transferring personal data**

You must ensure that data is kept as safe as possible when transferring data from one place to another and from one person to another (this includes when passing very sensitive information to camp officers etc).

**Key principles:**

* Only pass personal and sensitive information on to people who have authority to receive it.
* Always explain to the recipient what to do with the information and how to store it.
* If you are transferring personal or sensitive information in an electronic form, always use an encrypted EMW memory stick.
* If you are transferring personal or sensitive information in paper form, always keep in an envelope marked private and keep safe and secure on your person.
* If you are carrying personal and sensitive information (electronic or paper) always keep in a locked compartment in the car (e.g. boot) and never leave unattended unless locked (e.g. in your house in the evening).
* Never use social media to send personal or sensitive data.
* If you are discussing a particular sensitive case, make every effort to use verbal communication.

**Sending personal and sensitive data in emails:**

* Avoid sending personal and sensitive data in emails if at all possible (e.g. OneDrive can be used to transfer data between staff), remember it is much harder to control information sent over email.
* If you send sensitive information via email, you must mark the email as confidential.
* Once the email has been sent, delete the email from your sent items immediately.
* As you will always be passing sensitive information to a CCiW representative (volunteer or trustee) give clear instructions as to how they should treat the data and use the following sentence:

*This email contains personal and/or sensitive information. It has been passed on to you with permission from the office manager and we therefore ask you to delete the email as soon as possible. We remind you of your responsibilities as a CCiW representative to treat the information in line with the guide that you’ve been given. If you believe that this information has been seen by another individual, please contact the sender immediately to notify CCiW of this.*

**Receiving personal and sensitive data in an email:**

* When receiving information make sure that you copy information into an appropriate programme (e.g. word or adobe) and save the information on your device.
* Delete the email as soon as possible.
* If you are replying, do not include the original attachment or content in the email.

**Transferring personal and sensitive information for camps and conferences:**

* Transfer information in paper form if possible;
* Explain clearly to the recipient how they should handle the data;
* Use royal mail signed for service to send information through the post;
* Make sure you receive the paper forms back from officers and leaders, so that you can ensure that the data is destroyed in the office by appropriate means.

**Key Concept!**

***Take extra care when transferring data – this is when it’s most vulnerable.***

**Guidelines for using personal data**

As an organisation we will try and limit the use of personal and sensitive data by CCiW field staff and volunteers as much as possible. Field staff and volunteers will be directed to a trustee if at all possible to deal with requests relating to personal data.

It is your responsibility to work with trustees to ensure that data is used for the purpose it was collected. This means that:

* You should always use appropriate programmes to contact and use information:
  + Use Campaign monitor to send marketing and information emails;
  + Use the Bcc function to send group emails to committees and volunteers;
  + Never use social media to send marketing information to specific groups that you have created;
  + Use your Office 365 package to store and communicate data.
* Make sure you understand why you can contact a specific mailing/emailing list before you send the mailing.
* Make sure you use the correct templates to contact individuals.
* Never use information to do something that you have not received specific consent to do.
* Never pass information to third parties.
* Never pass information to volunteers unless you’ve been given permission to do so by an office manager.
* Take care when using the information – you can often store details without noticing it – e.g. a mail-merge, a paper scribble list. Make sure you delete all data correctly.

**Key Concept!**

***Never use information to do something that you’ve not been given permission to do.***

**Disposing of data**

We must take special care when disposing of data both electronically and in paper format.

Make sure you are aware of the retention policy relating to the data you are dealing with.

**Paper format:**

* Make sure you dispose of personal or sensitive data by shredding correctly.

**Electronic format:**

* Make sure you delete files and emails from your computer. This includes:
  + Trash Recycling bin
  + Sent folders
  + Online backups

**Data sent to volunteers:**

* Make sure you keep a log of what you send to volunteers and when it’s returned (if you need it returned).
* Dispose of this information correctly.

**Old equipment**

* If you believe that information could be stored on old equipment (e.g. old computer), make sure all data is deleted.

**Key Concept!**

***Keep your work environment tidy and dispose of information as soon as possible.***

**Reporting a breach**

One of the most important aspects of the new legislation is our responsibility to monitor our data and make sure that it’s not shared/stolen/lost/used for something it shouldn’t.

We must therefore be able to identify any situation where this happens and report it to the relevant authorities. This is called a data breach, and we could be fined heavily if we don’t respond correctly to a data breach.

A data breach occurs where personal data is compromised in any way. This includes:

* Data being destroyed or corrupted where it should not have been (e.g. your laptop is ruined by water damage, and you have not backed up your hard disk).
* Data being lost (e.g. your laptop is stolen; you misplace a USB-drive containing data; you are unable to find a paper file containing personal data).
* Data is unlawfully accessed (e.g. your email account is hacked; a third party takes an unauthorised copy of your data).
* Data being made publicly available without consent, whether intentionally or by accident. (e.g. failing to use BCC in email correspondence). When sending an email to multiple recipients you must use BCC unless they work for the EMW.

If you suspect a data breach has occurred, you must report this to the trustees immediately.

CCiW is required by law to report breaches to the Information Commissioner (ICO) within 72 hours of discovering the breach, and faces serious repercussions if it fails to do so.

Where a breach has occurred, a trustee will guide you through an assessment to judge any action that needs to be taken to protect the individuals involved.

**Key Concept!**

***You must tell us if you suspect anything.***