Maidenhead Care

Data Protection Policy and Procedures

Contents

REGISTERED CHARITY No. 1134263 REGISTERED COMPANY No. 6996751

www.maidenheadcare.org.uk Email: office@maidenheadcare.org.uk

Maidenhead Care

Data Protection Policy and Procedures

1.What is a Data Protection Policy and why do we need one?

(In this document, use of "us", "we" "our" and "Care" all refer to Maidenhead Care).

Having a Data Protection Policy is a legal requirement under the General Data Processing regulations (GDPR). We should also be interested for two reasons:

- **First the carrot:** the legislation contains sensible provisions to make life better for all. By ensuring compliance we should be improving the quality of experience that people have when they engage with Maidenhead Care.

- **Second the stick**: there are substantial fines for non-compliance.

The legislation set out in the GDPR provides organisations with a large amount of flexibility in how they comply. The purpose of this document is to explain how we comply with these principles.

2.What is the difference between a Data Protection Policy and a Privacy Policy?

This Data Protection Policy is primarily an internal document to help Care as an organisation ensure we comply with data protection legislation.

Under the legislation, there is also a requirement to provide a privacy notice to individuals when processing their personal data. The Care privacy notice is provided on our website http://www.maidenheadcare.org.uk/ and contains further details of our personal data handling policies.

3.What do we need to know?

GDPR consists of 99 Articles, and for the interpretation of the GDPR 173 Recitals. As a small charity, not everything in the new legislation is relevant to us, but we do need to be aware of certain key points.

4.Principle-based not rule-based

The earlier Data Protection Act 1998 was a principle-based legal structure and the GDPR continues that approach. This means that rather than a set of rigid rules, the law gives broad principles that will be applied differently by different organisations depending on their circumstances.

5.To process data we need a lawful basis

The GDPR sets out six lawful bases for processing personal data. Our Privacy Notice sets out those that are relevant to our operation. The biggest change in legislation Is consent. Consent means offering people genuine choice and control over how we use their data and the new rules are much clearer about exactly what this means.

REGISTERED CHARITY No. 1134263 REGISTERED COMPANY No. 6996751

www.maidenheadcare.org.uk Email: office@maidenheadcare.org.uk

Under GDPR, consent must be:

- Unbundled - separate from general terms and conditions
- Active opt-in - no pre-ticked boxes
- Named - clear who is given consent'
- Documented - records to be kept of the consent
- Easy to withdraw

6.Collecting client and volunteer information

When we collect this information, we must give a clear option about whether or not they give consent for their data to be processed and for what purposes. If we don't get consent at this point, through a clear opt-in, then we don't have permission to use that data. For this reason, all clients phoning for help in the future will be asked for permission to give their consent. Similarly, all volunteers will have received a consent form asking for permission to send them communications from Care.

7.Storing information

Storing information securely is already important and will only become more so. GDPR requires us to keep records demonstrating that our clients and volunteers have actively opted in. This has required our database system used to record client data to be updated and it now contains the date that permission was granted. The paper consent forms from volunteers are also safely stored for future reference.

8.Communications

When we send out communications we need to be confident that they have opted-in to the particular type of communication we are about to send.

We must also be confident that we are giving volunteers a simple way to opt out of receiving communications. For email newsletters, this should come in the form of an 'unsubscribe' or 'manage preferences' instruction at the bottom of the email.

9.Existing clients and volunteers

GDPR applies to historical data, not just future data that is collected after GDPR comes into force. This is why we have contacted all our volunteers to ensure that they have actively opted-in to receiving our communications and we will seek consent from existing clients for all new jobs as they are received.

10.Data use

Within Care, the master record of personal information of client and volunteer data is primarily held on the laptop used by Duty Officers (DO). To enable Care to function it is accepted that limited personal data will be passed to volunteers. This data will then be held in private homes and should be protected as far as is practicable. Never reveal such personal data that has been provided to any third parties. A further secure password

REGISTERED CHARITY No. 1134263 REGISTERED COMPANY No. 6996751

www.maidenheadcare.org.uk Email: office@maidenheadcare.org.uk

protected computer operated by the treasurer is used for back up of this data. The transfer of weekly data from the laptop to his system is by encrypted USB stick. This data is then backed up to our cloud provider.

11.Data Accuracy

We need to take all reasonable steps to ensure personal data is kept up to date and that it is accurate. For instance, by confirming a client's details when they call. If there is any doubt about the accuracy of personal data, then it should not be used.

12.Data Security

The Duty Officer's laptop is password protected and runs the latest operating system and is kept up to date at all times with relevant service upgrades. An industry standard anti-virus program and firewall are installed and kept up to date with upgrades. The password should be kept secure and separate from the laptop. The laptop is hand carried between Duty Officers and should be kept secure at all times. No connection from the laptop to the internet or any network is permitted.

A further secure password protected computer operated by the treasurer is used for back up and the transfer of weekly data from the laptop to this system is by encrypted USB stick. Such data is then then further backed up to our cloud provider.

Please bear in mind that email is not necessarily confidential or secure so should not be used for potentially sensitive communications.

13.Data Removal or Amendment

Care do not have an automatic system to respond to "Subject Access Requests" (see page 6). All such requests should be referred to the treasurer for action as appropriate.

14.Do we need a Data Protection Officer?

It is our opinion, and in line with most small charities, that this role is not required in Care. The responsibility for data protection will be undertaken collectively by the trustees. This decision will be reviewed if circumstances change.

15.Do we need to register with the ICO?

Care are not required to register with the ICO but we can register informally and it is likely this will happen.

16.ePrlvacy Regulation - changes to cookie compliance

The new ePrivacy Regulation has yet to be issued but it looks likely that it will enhance restrictions in tracking user behaviour often done through 'cookies'. The Care website no longer uses cookies.

REGISTERED CHARITY No. 1134263 REGISTERED COMPANY No. 6996751

www.maidenheadcare.org.uk Email: office@maidenheadcare.org.uk

17.Personal Data Breach

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

18.Responding to a personal data breach

If volunteers suspect, or are aware of such an event, they should contact the Duty Officer or a trustee of Care. They will review the situation and decide on what action is required. Any breach must be recorded even if it is not reportable. The ICO (Information Commissioners Office) have to be notified of a breach if the breach is likely to result in "a risk to the rights and freedoms of individuals". Like so much of GDPR, this is a judgement call as to when a data breach meets this threshold.

An example, if there is a breach and volunteer bank details are stolen this would certainly qualify as a breach that should be reported to the ICO. However, if there was a breach and a document containing only the names of a few volunteers was lost, then it is unlikely that this would need to be reported.

19.What to include in the breach report to the ICO

Article 33 of GDPR says you have to include specifics in a breach report, including:

- Details about the number of people and records involved.
- The categories of personal data involved.
- Name of the person within Care dealing with the issue.
- Description of the likely consequences of the breach.
- A description of how Care intend to deal with the breach.

Reports must be submitted within 72 hours of Care becoming aware of the breach.

20.Do we have to tell the affected people about a Data Breach?

This is covered by Article 34 of GDPR, if a data breach results in a "high risk to the rights and freedoms" of volunteers or clients Care have to inform those involved without "undue delay".

21.What training is available?

Care will arrange suitable training either through short workshops, on a one to one basis, or by the use of video particularly when new Duty Officers or Section Leaders take up positions.

It is hoped to include in future Care email newsletters, practical data protection issues like clearing out old information, keeping their access passwords secure, etc.

REGISTERED CHARITY No. 1134263 REGISTERED COMPANY No. 6996751

www.maidenheadcare.org.uk Email: office@maidenheadcare.org.uk

22.Subject Access Requests

Subject Access Requests (SAR) from volunteers and clients enable them to access their personal data or have it removed from our records.

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

- Request access to their personal information
- Update their own personal data to keep it accurate.
- Request deletion of their personal data.
- Request that their data be delivered to themselves or a 3rd party.

To process such requests, it may be necessary to verify the identity of the applicant. In such cases we will need proof of identity before we can exercise these rights. Once we have received a request we have to respond within one month. We need a system for managing changes in preferences when requested by either volunteers or clients. A manual approach is to be used at least for the time being where such requests would be actioned by the treasurer.

23.Disposal of Records

Care has a policy to keep financial records for a minimum period of 7 years to support HMRC audits. We endeavour to keep data only for as long as we need it. This means that we may delete it when it is no longer needed. When discarding paper records that contain personal data please treat them as confidential and dispose of them ideally by shredding. Similarly, any unnecessary or out of date electronic records should be deleted.

24.Data Protection Impact Assessment (DPIA)

A DPIA is a process that we are required to undertake to help us identify and minimise the data protection risks of any new major project that we may undertake which requires the processing of personal details. Any such DPIA will be prepared by the trustees and the details recorded for future reference.

25.Follow up and policy review

The date of this policy is noted on the last page. The policy will be reviewed regularly by the trustees and updated as necessary.

26.Contact details

You can contact the Information Commissioners Office on 0303 123 1113 or via email: https://ico.org.uk/global/contact-us/email/ or Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF Tel: 0303 123 1113 (local rate)

.

Date of Issue: 25/5/2019 Issue 1

.

|

1. GENERAL PRIVACY NOTICE

Our General Privacy Notice will be found on our web page:
vAArw.burchettsgreenparish.org

2. PARISH AND CHURCH SECURITY

- It is important that all data is kept safe and locked away. Data should be kept in locked

cupboards within locked offices, in Safes and in areas of churches that can be locked.

•The security of keys must be addressed, and a register of key holders maintained.

• Computers must have password protection and be subject to regular software updates.

• To make sure that all sensitive information whether financial, administration or personal is

identified and procedures put in place to protect that data from mis use.

3. DATA HELD OUTSIDE OF OFFICE AND CHURCH.

it is accepted that some data will be held in private homes. We will Identify the most sensitive

data and make sure this is always placed and stored in the Church office or Church. Other data

held in the home should be protected as far as is practicable.

4. CONSENT FORM.

Burchetts Green Parish will gain permission to save personal data and use that data as agreed by

the individual. We will seek that permission through a Consent Form and retain that form in the

office. The individual may OPT OUT of that permission at any time by notifying the Parish Office.

An OPT OUT option will be inserted into all email communications.

5. EMAILS

Burchetts Green Parish will subscribe to an external Church Management software system which

will enable the following functions to be fulfilled.

• A Parish Data Base of all contacts.

•

Each Officer or coordinator will have access via a User name and Password, to that area of the data base that they are entitled to access.

•

Each Officer or coordinator will have a dedicated email address which can be accessed through this Computer Management software. The external Management will allow for the sending and receiving of emails using the dedicated BG email address.(example: richard.m@bgparish.org)

• All emails containing more than one recipient should use the Bcc facility to hide email addresses.

•

On leaving office, the dedicated user name and password will be removed.

6. TIMEFRAME AND REVIEW.

The recommended retention period for data Is 7 years. Burchetts Green Parish will, on a regular

basis, review the retained data and securely dispose of all unnecessary data.

7. DATA PROTECTION TRAINING.

We will arrange suitable training either through short workshops,

on a one to one basis or by the

use of Video as Is required and on a regular basis where new Officers or Coordinators take up

positions.

POLICY ON DELETE ; REQUEST DATA; DATA SECURITY

17*^ April 2018.

Responsibilities

Everyone who works for or with [company name] has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

The board of directors is ultimately responsible for ensuring that [company name] meets its legal obligations.

General staff guidelines

The only people able to access data covered by this policy should be those who need it for their work.

Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.

[Company name] will provide training to all employees to help them understand their responsibilities when handling data.

Employees should keep all data secure, by taking sensible precautions and following the guidelines below.

In particular, strong passwords must be used and they should never be shared.

Personal data should not be disclosed to unauthorised people, either within the company or externally.

REGISTERED CHARITY No. 1134263 REGISTERED COMPANY No. 6996751

www.maidenheadcare.org.uk Email: office@maidenheadcare.org.uk

Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.

Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data controller.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

Data should be **protected by strong passwords** that are changed regularly and never shared between employees.

If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used.

Data should only be stored on **designated drives and servers**, and should only be uploaded to an **approved cloud computing services**.

Servers containing personal data should be **sited in a secure location**, away from general office space.

Data should be **backed up frequently**. Those backups should be tested regularly, in line with the company's standard backup procedures.

Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.

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

Data use

Personal data is of no value to [company name] unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

When working with personal data, employees should ensure **the screens of their computers are always locked** when left unattended.

Personal data **should not be shared informally**. In particular, it should never be sent by email, as this form of communication is not secure.

Data must be **encrypted before being transferred electronically**. The IT manager can explain how to send data to authorised external contacts.

Personal data should **never be transferred outside of the European Economic Area**.

Employees **should not save copies of personal data to their own computers.** Always access and update the central copy of any data.

Data accuracy

The law requires [company name] to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort [company name] should put into ensuring its accuracy.

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

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- [Company name] will make it easy for data subjects to update the information [company name] holds about them. For instance, via the company website.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
- It is the marketing manager's responsibility to ensure marketing databases are checked against industry suppression files every six months.

Subject access requests

All individuals who are the subject of personal data held by [company name] are entitled to:

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

If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the data controller at [email address]. The data controller can supply a standard request form, although individuals do not have to use this.

Individuals will be charged £10 per subject access request. The data controller will aim to provide the relevant data within 14 days.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, [company name] will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Providing information

[Company name] aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company.

[This is available on request. A version of this statement is also available on the company's website.]

YOUR DATA

Your company has a list of all types of personal information it holds, the source of that information, who you share It with, what you do with it and how long you will keep it Data Processor Data Controller

Your company has a list of places where It keeps personal Information and the ways data flows between them Data Processor Data Controller

Your company has a publicly accessible privacy policy that outlines all processes related to personal data. Data Processor Data Controller

Your privacy policy should Include a lawful basis to explain why the company needs to process personal Information

ACCOUNTABILITY & MANAGEMENT

Your company has appointed a Data Protection Officer (DPO) Data Processor Data Controller

Create awareness among decision makers about GDPR guidelines

Data Processor Data Controller

Make sure your technical security is up to date.

Data Processor Data Controller

Train staff to be aware of data protection

You have a list of sub-processors and your privacy poiicy mentions your use of this sub-processor sz

Data Processor

REGISTERED CHARITY No. 1134263 REGISTERED COMPANY No. 6996751

www.maidenheadcare.org.uk Email: office@maidenheadcare.org.uk

If your business operates outside the EU, you have appointed a representative within the EU.

You report data breaches involving personal data to the local authority and to the people (data subjects) involved Data Processor Data Controller

There is a contract in place with any data processors that you share data with

NEW RIGHTS

Your customers can easily request access to their personal Information V

Your customers can easily update their own personal information to keep it accurate

You automatically delete data that your business no longer has any use for

Your customers can easily request deletion of their personal data

Your customers can easily request that you stop processing their data

Your customers can easily request that their data be delivered to themselves or a 3rd party

Your customers can easily object to profiling or automated decision making that could impact them

Data Controller

CONSENT

Ask consent when you start processing a person's information

Your privacy policy should be written in clear and understandable terms

it should be as easy for your customers to withdraw consent as it was to give it in the first place

if you process children's personal data, verify their age and ask consent from their legal guardian

When you update your privacy policy, you inform existing customers

FOLLOW-UP

You regularly review policies for changes, effectiveness, changes in handling of data and changes to the state of affairs of other countries your data flows to. ^

SPECIAL CASES

Your business understands when you must conduct a DPIA for high-risk processing of sensitive data.

You should only transfer data outside of the EU to countries that offer an appropriate level of protection

Ten rules for data protection compliance

1. Consent
2. Sensitive data
3. Individual rights
4. Review files

5. Disposal of records

6. Accuracy

7. Security

8. Disclosing data

9. Worldwide transfer

10. Third party processors

Our terms and conditions, and the privacy notices below, are all written to be fully compliant with European privacy and data regulations (GDPR). It's all written in language that is designed to be understood and read by a 'normal' (apologies lawyers) person.

But to help you along, here are the basics - for us it isn't just the letter of the law that applies here, it is the spirit and principles we take seriously, to protect your data and your contract with us:

REGISTERED CHARITY No. 1134263 REGISTERED COMPANY No. 6996751

www.maidenheadcare.org.uk Email: office@maidenheadcare.org.uk