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