Bexhill Maritime

Registered Charity No. 1203659

Data Protection (GDPR) Policy

Introduction

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the European Council and the European Commission intend to strengthen and unify data protection for individuals within the European Union (EU). It also addresses the export of personal data outside the EU. The primary objectives of the GDPR are to give people back control of their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. The Regulations cover both written and computerised information and the individual's right to see such records.

Bexhill Maritime CiO needs to collect data, including some personal information, in order to carry out its' work.
Bexhill Maritime CiO is exempt from registering with the ICO and is not required by law to have a data protection officer, however our organisation regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal, and we intend to ensure that personal information is treated lawfully and correctly. We expect all of our staff and volunteers to comply with GDPR and training will be available accordingly.

Community Supporters CiO will undertake regular information audits to find out what data we hold and what we do with it. We will put ourselves in the position of the people we're collecting information about, and are working towards GDPR compliance, having updated our policies and procedures as required.

Where we hold personal information about our service users or volunteers, we protect that information by:
• only collecting information that we need for a specific purpose;
• keeping it secure;
• limiting access to it to only those with a strict need to know;
• ensuring it is relevant and up to date;
• only holding as much as we need, and only for as long as we need it; and
• allowing the subject of the information to see it on request.
We always seek informed consent to collect personal data.

Definitions

Processing of information – how information is held and managed.
Information Commissioner – formerly known as the Data Protection Commissioner.
Notification – formerly known as Registration.
Data Subject – used to denote an individual about whom data is held.
Data Controller – used to denote the entity with overall responsibility for data collection and management. Community Supporters CiO is the Data Controller for the purposes of the Act.
Data Processor – an individual handling or processing data.
Personal data – any information which enables a person to be identified.
Special categories of personal data – information under the Regulations which requires the individual's explicit consent for it to be held by the Company.

Data Protection Principles

As data controller, Community Supporters CiO is required to comply with the principles of good information handling.

These principles require the Data Controller to:

1. Process personal data fairly, lawfully and in a transparent manner.
2. Obtain personal data only for one or more specified and lawful purposes and to ensure that such data is not processed in a manner that is incompatible with the purpose or purposes for which it was obtained.
3. Ensure that personal data is adequate, relevant and not excessive for the purpose or purposes for which it is held.
4. Ensure that personal data is accurate and, where necessary, kept up to date.
5. Ensure that personal data is not kept for any longer than is necessary for the purpose for which it was obtained.
6. Ensure that personal data is kept secure.
7. Ensure that personal data is not transferred to a country outside the European Economic Area unless the country to which it is sent ensures an adequate level of protection for the rights (in relation to the information) of the individuals to whom the personal data relates.

The Rights of an Individual

Under the Regulations a Data Subject has the following rights with regard to those who are processing his/her data:
• The right to be informed
• The right of access
• The right to rectification
• The right to erasure

• The right to restrict processing
• The right to data portability
• The right to object
• Rights in relation to automated decision making and profiling
• The right to lodge a complaint with a supervisory authority

Personal and special categories of personal data cannot be held without the Data subject's consent (however, the consequences of not holding it can be explained and a service withheld).

Data cannot be used for the purposes of direct marketing of any goods or services if the Data Subject has declined their consent to do so.

Data Subjects have a right to have their data erased and to prevent processing in specific circumstances:
• Where data is no longer necessary in relation to the purpose for which it was originally collected
• When a Data Subject withdraws consent
• When a Data Subject objects to the processing and there is no overriding legitimate interest for continuing the processing
• Personal data was unlawfully processed

A Data Subject has a right to restrict processing – where processing is restricted, Community Supporters CiO is permitted to store the personal data but not further process it. Community Supporters CiO can retain just enough information about the individual to ensure that the restriction is respected in the future.

A Data Subject has the 'right to be forgotten'.
Data Subjects can ask, in writing to the Directors or the Project Coordinator, to see all personal data held on them, including e-mails and computer or paper files. The Data Processor (Community Supporters CiO) must comply with such requests within 30 days of receipt of the written request.

Consent

Community Supporters CiO must record service users' explicit consent to storing certain information (known as 'personal data' or 'special categories of personal data') on file.

For the purposes of the Regulations, personal and special categories of personal data cover information relating to:

1. The racial or ethnic origin of the Data Subject.
2. His/her political opinions.
3. His/her religious beliefs or other beliefs of a similar nature.

4. Whether he/she is a member of a trade union.
5. His/her physical or mental health or condition.
6. His/her sexual life.
7. The commission or alleged commission by him/her of any offence.
8. Online identifiers such as an IP address.
9. Name and contact details.
10. Genetic and/or biometric data which can be used to identify an individual.

Consent is not required to store information that is not classed as special category of personal data as long as only accurate data that is necessary for a service to be provided is recorded.

Community Supporters CiO will always seek consent where personal or special categories of personal information is to be held.

It should also be noted that where it is not reasonable to obtain consent at the time data is first recorded and the case remains open, retrospective consent should be sought at the earliest appropriate opportunity.

Obtaining Informed Consent

Informed consent is when
• An Individual/Service User clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data,
• And then gives their consent.
Consent obtained for one purpose cannot automatically be applied to all uses e.g. where consent has been obtained from a service user in relation to information needed for the provision of that service, separate consent would be required if, for example, direct marketing was to be undertaken.

Specific consent for use of any photographs and/or videos taken should be obtained in writing. Such media could be used for, but not limited to, publicity material, press releases, social media, and website. Consent should also indicate whether agreement has been given to their name being published in any associated publicity. If the subject is less than 18 years of age then parental/guardian consent should be sought.

Individuals have a right to withdraw consent at any time.

How we Ensure Informed Consent

Community Supporters CiO will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form.

When collecting data, Community Supporters CiO will ensure that the Individual/Service User:

a) Clearly understands why the information is needed
b) Understands what it will be used for and what the consequences are should the Individual/Service User decide not to give consent to processing
c) As far as reasonably possible, grants explicit written consent for data to be processed
d) Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress
e) Has received sufficient information on why their data is needed and how it will be used

We provide individuals with the following privacy information:

• The name and contact details of our organisation.
• The purposes, lawful basis, and retention periods for personal information, as well as who has access to it and how it is kept.
• The details of transfers of the personal data to any third countries or international organisations.

We have a privacy statement on any form requesting personal information. We give individuals information regarding:
• Why we need the data
• What we will do with it
• How it will be stored
• Who will have access to it
• The retention period and how and when it will be destroyed when no longer needed
• How they can withdraw consent

We provide individuals with privacy information at the time we collect their personal data from them.
We do not obtain personal data from a source other than the individual.
We provide information in a way that is concise, transparent, intelligible, easily accessible and we use clear and plain language.

Disclosure

Community Supporters CiO may share some data with other agencies such as the local authority, funding bodies and other voluntary agencies, however all data will be anonymised unless we require consent to share personal information, which we will obtain first, or unless there is a safeguarding issue (please see our separate safeguarding policy).

The Individual/Service User will be made aware how and with whom their information will be shared. There are circumstances where the law allows Community Supporters CiO to disclose data (including sensitive data) without the data subject's consent.
These are:

a) Carrying out a legal duty or as authorised by the Secretary of State
b) Protecting vital interests of an Individual/Service User or other person
c) The Individual/Service User has already made the information public
d) Conducting any legal proceedings, obtaining legal advice or defending any legal rights
e) Monitoring for equal opportunities purposes – i.e. race, disability or religion
f) Providing a confidential service where the Individual/Service User's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill Individuals/Service Users to provide consent signatures.
Consent will be sought wherever possible.

Use of Files, Books and Paper Records

In order to prevent unauthorised access or accidental loss or damage to personal information, it is important that care is taken to protect personal data. Paper records should be kept in locked cabinets/drawers overnight and care should be taken that personal and special categories of personal information is not left unattended and in clear view during the working the day. If your work involves you having personal / and/or special categories of personal data at home or in your car, the same care needs to be taken.

Disposal of Scrap Paper, Printing or Photocopying Overruns

Be aware that names/addresses/phone numbers and other information written on scrap paper are also considered to be confidential. Please do not keep or use any scrap paper that contains personal information but ensure that it is shredded.

If you are transferring papers from your home to the office for shredding this should be done as soon as possible and not left in a car for a period of time. When transporting documents, they should be carried out of sight in the boot of your car.

Computers

Where computers are networked, access to personal and special categories of personal information is restricted by password to authorised personnel only.

Computer monitors in public areas should be positioned in such a way so that passers-by cannot see what is being displayed. If working in a public area you should lock your computer when leaving it unattended.

Firewalls and virus protection to be employed at all times to reduce the possibility of hackers accessing our system and thereby obtaining access to confidential records.

Documents should only be stored on the server or cloud-based systems and not on individual computers.

Where computers or other mobile devices are taken for use off the premises the device must be password protected.

Cloud Computing

When commissioning cloud-based systems, Community Supporters CiO will satisfy themselves as to the compliance of data protection principles and robustness of the cloud-based providers.

Direct Marketing

Direct Marketing is a communication that seeks to elicit a measurable fundraising response (such as a donation, a visit to a website, etc.). The communication may be in any of a variety of formats including mail, telemarketing and email. The responses should be recorded to inform the next communication. Community Supporters CiO will not share or sell its database(s) with outside organisations.

Community Supporters CiO may hold email addresses of our staff, volunteers, service users and other supporters, to whom we will from time to time send copies of our newsletters, newspaper and details of other activities that may be of interest to them. Specific consent to contact will be sought from our staff, service users and other supporters, including which formats they prefer (e.g., mail, email, phone etc.) before making any communications.

We recognise that clients, staff, volunteers and supporters for whom we hold records have the right to unsubscribe from our mailing lists. This wish will be recorded on their records and they will be excluded from future contacts.

Personnel Records

The Regulations apply equally to volunteer and staff records. Community Supporters CiO may at times record special categories of personal data with the volunteer’s consent or as part of a staff member’s contract of employment.

For staff and volunteers who are regularly involved with vulnerable adults, it will be necessary for Community Supporters CiO to apply to the Disclosure & Barring Service to request a disclosure of spent and unspent convictions, as well as cautions, reprimands and final warnings held on the police national computer. Any information obtained will be dealt with under the strict terms of the DBS Code. Access to the disclosure reports is limited to the Project Coordinator and Directors. If there is a positive disclosure the Directors will discuss this, anonymously, with the Project Coordinator and our insurers to assess the risk of appointment. Directors and insurers should not see the report itself, only the Project coordinator will have access to this.

Confidentiality

When working from home, or from some other off-site location, all data protection and confidentiality principles still apply. All computer data, e.g., documents and programmes related to work for Community Supporters CiO should not be stored on any external hard disk or on a personal computer.

Workstations in areas accessible to the public, e.g., reception or trading office, should operate a clear desk practice so that any paperwork, including paper diaries, containing personal and/or special categories of personal data is not left out on the desk where passers-by could see it.

When sending emails to outside organisations, care should be taken to ensure that any identifying data is removed and that initials are to be used. Confidential and/or special categories of personal information should be written in a separate document which should be password protected before sending. This document should be highlighted as confidential.

Any paperwork kept away from the office should be treated as confidential and kept securely as if it were held in the office. Documents should not be kept in open view (e.g., on a desktop) but kept in a file in a drawer or filing cabinet as examples, the optimum being a locked cabinet but safely out of sight is a minimum requirement.

If you are carrying documents relating to staff, volunteers or service users you should keep the documents locked out of sight in the boot of the car (not on the front seat). When carrying paper files or documents they should be in a locked briefcase or in a folder or bag which can be securely closed or zipped up. The briefcase/folder/bag should contain Community Supporters CiO contact details. Never take more personal data with you than is necessary.

Retention of Records

Paper records should be retained for the following periods at the end of which they should be shredded:

• Client records – 6 years after ceasing to be a client.
• Staff records – 6 years after ceasing to be a member of staff.
• Unsuccessful staff application forms – 6 months after vacancy closing date.
• Volunteer records – 6 years after ceasing to be a volunteer.
• Timesheets and other financial documents – 7 years.
• Employer's liability insurance – 40 years.
• Other documentation as it is no longer needed for the task in hand.

Archived records should clearly display the destruction date.

What to Do If There Is a Breach

If you discover, or suspect, a data protection breach you should report this to the Project Coordinator and/or the Directors who will decide whether it needs to be reported to the Information Commissioner and take actions to prevent a reoccurrence. There is a time limit for reporting breaches to ICO so the breach must be reported without delay. The Data Subject involved will also be informed.

Any deliberate or reckless breach of this Data Protection Policy by an employee or volunteer may result in disciplinary action which may result in dismissal or the instigation of our Letting Go of Volunteers Policy.

Powers of the Information Commissioner

The following are criminal offences, which could give rise to a fine and/or prison sentence

• The unlawful obtaining of personal data.
• The unlawful selling of personal data.
• The unlawful disclosure of personal data to unauthorised persons.

Details of the Information Commissioner

Further information is available at www.ico.org.uk

The Information Commissioner's office is at:
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

Switchboard: 01625 545 700
Email: mail@ico.gsi.gov.uk

Implementation and Quality Assurance

Implementation is immediate and this Policy shall stay in force until any alterations are formally agreed by Directors. This Policy will be reviewed annually by the Directors, sooner if legislation, best practice or other circumstances indicate this is necessary.

All aspects of this Policy shall be open to review at any time.

Policy adopted: August 18th, 2023

Updated:

Review date: July, 2025