Data Protection and Privacy Policy

Contents:

DOCUMENT OWNER

Data Protection Officer – Ian Fletcher

APPROVED BY

Chairman of the Trustees – Philip Shepperd

VERSION HISTORY

Version Number	Amendments	Date of Issue
1.0	Initial Issue	June 2018

1. Purpose and aims

Sidmouth Lifeboat, in carrying out its duties as a Declared Rescue Facility, will gather, use and retain personal information on its employees, volunteers and members of the public to support operational and public engagement activities. Where necessary, this can include the processing of personal data of prospective members, casualties, other partner emergency service agencies, and any other person or people the Charity has a relationship with or may need to do so.

Personal data may include personal and family details, lifestyle and social circumstances, financial, education and employment details. Where required, the organisation may be required to process sensitive classes of information such as physical and mental health details, racial or ethnic origin, religious or other beliefs of a similar nature.

This policy exists to ensure that all members of Sidmouth Lifeboat:

- Complies with data protection law and follow good practice
- Protects the rights of individuals whose data is used
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

2. General Data Protection Regulations and Data Protection Act

The new Data Protection Act (DPA), which comes into force on 25th May 2018, will require organisations that control the processing of personal data, which includes Sidmouth Lifeboat, to be much more open and transparent with how they handle personal data regardless of whether it stored electronically or in hard copy.

Personal data is data which relates to a living individual which allows that individual to be identified. Sensitive personal data means personal data consisting of information as to racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health or condition, sexual life, actual or alleged criminal offence.

To comply with the law, personal information must be collected and used fairly and lawfully. It must also be managed in a secure manner. The DPA will be supported by the General Data Protection Regulation (GDPR) which lays out six principles for processing of personal data. These are:

- Lawfulness, fairness and transparency – Data should be gathered and used in a way that is legal, fair and understandable
- Purpose limitation – Organisations should only use data for a legitimate purpose specified at the time of collection
- Data minimisation – Data collected should be limited only to what is required for the purpose stated

- Accuracy – Data should be accurate and kept up to date
- Storage limitation – Personal data should be stored for as long as is necessary
- Integrity and confidentiality – Personal data should be held in a safe and secure way

3. Responsibilities and expectations

The policy applies to all members of Sidmouth Lifeboat and applies to all data they hold relating to an individual and can be linked directly to them. This may include, but not be limited to, names, phones numbers, email addresses and photographs.

All members of Sidmouth Lifeboat have some level of responsibility for ensuring data is collected, stored and handled appropriately. All members must ensure that they handle and process personal data in line with this policy and data protection principles.

The DPO is responsible for:

- Keeping members updated about data protection responsibilities, risks and issues
- Reviewing this policy as required
- Providing advice and handling data protection queries
- Dealing with any Subject Access or Freedom of Information Requests
- Dealing with any actual or suspected data breaches.

All Members are responsible for:

Only accessing personal data in carrying out their duties in relation to the purpose of the charity.

Keeping all data secure, by taking sensible precautions and following the guidelines within this policy.

Using password protection for documents and files where appropriate and ensuring passwords are kept secure.

Regularly reviewing personal data and updating it where necessary. If no longer required, it should be deleted and disposed of appropriately.

Securely destroying any personal data. This will mean using a shredder to dispose of hardcopy data, and ensuring the complete deletion of electronic records.

Reporting any breach or potential breach of personal data to the DPO as a matter of urgency and providing as much information as possible

4. Data storage

When personal data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it. When not required the paper or files should be kept in a locked drawer or filing cabinet. Members who are required to store paper copies of personal data should have access to the locked filing cabinet within the Boathouse. Members should make sure paper data is not left where unauthorised people could see them and should be shredded and disposed of securely when no longer required.

When personal data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts. Any personal data held electronically must Where a member is require to hold personal data on home computers, they must provide assurance to the DPO is responsible for ensuring those who handle personal data electronically provide evidence that such security controls are in place, including the provision of regular (monthly) secure encrypted backup. The Back The majority of The Team electronic data should be held on a secure Team system, such as Office 365, SharePoint, SARCALL and D4H (delete or add as appropriate) which are password protected and access is restricted. Where data is required to be held on a member's personal computer and/or mobile phone or where additional level of restriction of data held on The Team systems is required, these documents should be password protected.

5. Data retention

Sidmouth Lifeboat has a statutory duty to keep certain records for a minimum period of time. For example, casualty medical information is required to be kept for the following periods:

- Adults – 8 years
- Children – until 25th birthday
- Pregnant women – 25 years

Operational and Radio Log Books, which may contain personal data as part of a Coastguard initiated incident, are retained for xx years.

In other cases Sidmouth Lifeboat shall not keep personal data for longer than is necessary or as may be required by applicable law.

6. Data retention

Sidmouth Lifeboat will take all reasonable steps to ensure data is kept accurate and up to date. Members of Sidmouth Lifeboat are to ensure that their personal data held by the charity is kept accurate.

7. Subject Access and Freedom of Information Requests

Any individual may request the personal information that Sidmouth Lifeboat holds on them. Any such request should be made in writing to the DPO (including email) who will verify that the identity of the individual is the data subject before releasing any information.

Any Freedom of Information (FOI) request must also be made in writing (including email). The DPO will respond to any FOI as appropriate.

8. CCTV and Photography

CCTV

The Boathouse has CCTV installed to monitor the exterior and interior of the building 24 hours a day for the following purposes:

- To assist with the safety and well-being of Sidmouth Lifeboat members and visitors
- To deter and detect crime
- To assist in the identification, apprehension and prosecution of offenders

Where, in carrying out these purposes, images are obtained of persons committing acts of an illegal nature, these images may be used as evidence in criminal and/or legal proceedings.

Monitors showing live CCTV images are located in the kitchen area and upstairs crew room. These areas are restricted to members only.

Third party access and disclosure is permitted only if in accordance with the purpose for which the system is used and will be limited to:

- Police and other law enforcement or regulatory agencies, where the images recorded could assist in a specific enquiry or investigation
- Prosecution agencies
- Relevant legal representatives of people whose images have been recorded and retained
- In exceptional cases, to others to assist in identification of a victim, witness or perpetrator in relation to a criminal incident.

Images obtained by the CCTV system will be stored for a maximum of 30 days before being overwritten. Where an active investigation is ongoing images may be required to be retained for such longer period as is appropriate.

Photographs and video footage

Photographs and video footage will be taken for purposes of public relations and promoting the activities of the Lifeboat. Only members of Sidmouth Lifeboat (boat crew and support team) will be used in such imagery, unless a member specifically asks for their image not to be included. General photographs and/or footage taken

as part of an event or activity will not include members of the public, unless it is generic enough to minimise the opportunity for recognition.

9. Further information

Any questions or queries regarding this policy or data protection in general should be directed to the Sidmouth Lifeboat's DPO in the first instance.

Further external information can be found on the Information Commissioner's Office website www.ico.org.uk which provides more detail regarding some of the areas covered in this policy.