Data Protection Policy

Introduction

This policy outlines Wave Muswell CIO's ("Wave Hub's") commitment to data protection and compliance with the UK Data Protection Act 2018. The purpose of this policy is to ensure that all personal data held by the charity is processed lawfully, fairly, and transparently, and that the rights of data subjects are protected. This policy applies to all individuals working on behalf of Wave Hub, including trustees, staff, and volunteers.

It is worth highlighting by way of context that our need to know and retain personal data is relatively modest. For staff and volunteers we need to hold details of reference checks and payroll, and for core supporters, details of donations – but for customers and others, in most cases our need is limited to identification and contact details, and photographic images for promotional purposes.

Data Protection Lead

Wave Hub has an appointed Data Controller who is responsible for overseeing data protection and leading on any incident investigation and reporting. The Data Controller will also ensure that all staff and volunteers are provided with any induction, on the job or other training and made aware of their responsibilities.

Data Controller	Name: Steve Mersereau (steve@wavehub.org.uk)	Appointed: 1 December 2023

Data Protection

Data protection is the practice of safeguarding personal information by applying data protection principles and complying with the Data Protection Act, that regulates the processing of personal data. Wave Hub follows guidelines provided by The UK Information Commissioner's Office (ICO).

Our data protection principles

We work to ensure that data we hold is:

- **Processed lawfully, fairly and in a transparent manner.**
  - There are several grounds on which data may be collected, including consent.
  - We are clear that our collection of data is legitimate and we have obtained consent to hold an individual's data, where appropriate.
  - We are open and honest about how and why we collect data and individuals have a right to access their data.

- **Collected only for specified, explicit and legitimate purposes.**
  - We are clear on what data we will collect and why.
  - When data is collected for a specific purpose, it may not be used for any other purpose without the consent of the person whose data it is.

- **Adequate, relevant and limited to what is necessary.**
  - We collect all the data we need to get the job done.
  - We don't collect data that we don't need.

- **Accurate and, where necessary, kept up to date.**
  - We ensure that what we collect is accurate and have processes to ensure that data which needs to be kept up-to-date is maintained- eg volunteer records.
  - When we identify mistakes, we correct them promptly.

- **Kept for no longer than is reasonable and necessary.**
  - We understand what data we need to retain, for how long and why.
  - We only hold data only for as long as we need to.
  - That includes both hard copy and electronic data.
  - We have a review process to ensure data no longer needed is destroyed.

- **Processed to ensure appropriate security, not only to protect against unlawful use, but also loss or damage.**
  - Data is held securely, so that it can only be accessed by those who need it; we use Google Drive and share access details only with those who require them.
  - We operate a BYOD (bring your own device) policy for employees; we require that employees have anti-virus software installed.
  - Staff understand their responsibilities to safeguard against cyber-attack. The data controller conducts training once a year.
  - We use a password manager and the Data Controller is responsible for its administration.
  - We have back-up and disaster recovery processes to ensure that important data is recoverable if needed.

Use of Imagery/Video

All imagery is protected by copyright and cannot be used without the consent of the owner, usually the person who took the image. Particular care is to be taken when using images of children or other vulnerable people, and we may in some cases need to liaise with a responsible carer.

When taking photographs which may be used in publicity, we will inform people of our activity and ask that anyone wishing to avoid being photographed let us know, in which case we will endeavour to avoid using their image. In any case of doubt, we will err on the side of caution and obtain consent wherever this is reasonably possible.

Here are some helpful questions to consider when using imagery:

- For what purpose was the original image taken? If it was for one purpose, such as personal use, it cannot be used for another without the consent of the individuals concerned
- Is the image sensitive personal data? If it is, do you have the individual's consent?
- For small groups and individuals, has an image consent form been used?
- When using images of children, or people who may not be competent, do you have valid consent?
- When using images of children or other vulnerable people, are you confident your use of the image will not place them at risk? Particularly, if it is to be used publicly, such as in the Media or on the web.
- When photographing large groups, have the individuals been given a chance to opt out of the photograph?
- Has the person/people in the image been told how the image will be used?
- Are you using the image according to how the person/people were told or could reasonably expect it would be used?

Data Breach

A breach is more than only losing personal data. It is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

We will investigate the circumstances of any reported loss or breach, to identify if any action needs to be taken. Action might include changes in procedures, where these will help to prevent a recurrence, or disciplinary or other action, in the event of negligence.

If we consider that a breach is likely to result in a risk to the rights and freedoms of individuals, we will notify the ICO within 72 hours of becoming aware of it.

Fundraising

We will ensure that our fundraising complies with the Data Protection Act and ICO guidelines and also the Fundraising Regulator guidelines including, if applicable, direct marketing and Privacy and Electronic Communications Regulations (PECR), which govern electronic direct marketing.. We will respect the privacy and contact preferences of our donors and respond promptly to requests to cease contacts or complaints.

Version Control - Approval and Review

Version No	Approved By	Approval Date	Main Changes	Review Period
1.0	Board	Dec 23	Initial draft approved	Annually
1.1	Board	Apr 24	changes to section “Processed to ensure appropriate security”	Annually

This data protection policy will be reviewed and approved by the Trustees annually, and as part of any data breach investigations, to test that it has been complied with and to see if any improvements might realistically be made to it.