Wellbeing in the Weald

Information and Data Security Policy

1. Introduction

Wellbeing in the Weald is committed to protecting the personal data of its supporters, beneficiaries, staff, volunteers, and other stakeholders. This policy outlines the principles and procedures we follow to ensure the security and confidentiality of all personal data we handle.

Please refer to our Privacy Notice for the ways in which we use and share personal data.

2. Scope

This policy applies to all staff, volunteers, trustees, and anyone working on behalf of Wellbeing in the Weald. It covers all personal data we collect, process, and store, regardless of format (electronic or paper-based).

3. Legal Framework

This policy adheres to the following:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018

4. Key Data Security Principles

We uphold the following six data protection principles:

1. **Lawfulness, fairness, and transparency:** We collect and process data only for legitimate purposes with clear consent or another lawful basis. We are transparent about how we use data.
2. **Purpose limitation:** We collect data only for specific, clearly defined purposes and do not process it further in a manner incompatible with those purposes.
3. **Data minimisation:** We collect and process only the minimum personal data necessary for the intended purpose.
4. **Accuracy:** We take reasonable steps to ensure the data we hold is accurate and, where necessary, kept up to date.
5. **Storage limitation:** We retain data only for as long as necessary for the purpose it was collected or in accordance with legal requirements.
6. **Integrity and confidentiality:** We implement appropriate technical and organizational measures to ensure the security of personal data, protecting it

from unauthorized or unlawful processing, accidental loss, destruction, or damage.

5. Data Security Measures

We take the following measures to secure personal data:

- **Access controls:** Only authorised personnel have access to personal data on a need-to-know basis. Strong passwords and access controls are used for IT systems.
- **Data encryption:** Unless required in a more accessible format for any specific activity, ensure sensitive data is encrypted at rest and in transit.
- **Incident response:** We have procedures in place to identify, report, and address data breaches.
- **Cybersecurity awareness training:** Staff receive training on data security best practices to identify and prevent cyber threats.
- **Data retention and disposal:** We have guidelines for how long data is retained and a secure method for disposal of data that is no longer needed. Contact lists are reviewed every 3 years.

Staff, volunteers, trustees, and anyone working on behalf of Wellbeing in the Weald must:

- **Refer to the Hon Secretary and/or the Chair immediately in the event of any concerns about a potential data vulnerability or breach.**
- **Use strong passwords: Create strong and unique passwords for all your online accounts.**
- **Shared access: Keep a record of who has access to any shared passwords or accounts.**
- **Each activity Leader has a folder with emergency contact details for attendees, details are updated monthly by administrator and Hon Sec. Leaders are responsible for keeping the folder secure when activity is not taking place. Old details are shredded**.
- **Data / cyber security training for administrators, Leaders, and Hon Sec. should be reviewed regularly by Hon Sec.**
- **Be cautious about clicking on links or opening attachments: Be wary of suspicious emails or messages and avoid clicking on unknown links or attachments.**
- **Beware of phishing scams: Do not give out personal information through unsolicited emails or messages.**
- **Not share personal data or any sensitive information about Wellbeing in the Weald's operations, finances, beneficiaries, or donors without proper authorisation.**

- **Respond to any requests for removal of email and contact details from newsletter/email contact groups**
- **Volunteer contact lists to be reviewed every 3 years**

6. Data Subject Rights

Individuals have the following rights under the UK GDPR:

- Right to access their personal data
- Right to rectification of inaccurate data
- Right to erasure (right to be forgotten)
- Right to restrict processing
- Right to data portability
- Right to object to processing

Staff, volunteers, trustees, and anyone working on behalf of Wellbeing in the Weald must refer to the Hon Secretary and/or the Chair immediately in the event of any inquiry or request by any individual whose data we hold about any of the above rights.

7. Data Breaches

We will promptly investigate any suspected data breaches and notify the Information Commissioner's Office (ICO) if necessary. We will also inform affected individuals where appropriate.

8. Review and Update

This policy will be reviewed and updated regularly to reflect changes in data protection legislation and best practices.

9. Contact

For any questions or concerns regarding data security, please contact our Data Protection Officer (DPO) Seamus O’Brien at seamusobr@gmail.com