Alma Beacon is the operating name of Windsor Christian Action a registered charity in England No.1154308

Data Protection Policy

Introduction

This policy applies to Windsor Christian Action (operating name Alma Beacon) registered charity No. 1154308 and all its Projects ("the Charity").

1. The Charity needs to gather and use certain information about individuals. These can include guests, suppliers, business contacts, associates, employees, volunteers, Trustees and other people the Charity has a relationship with or may need to contact.

2. This policy describes how this personal data must be collected, handled and stored to meet the Charity's data protection standards — and to comply with the law.

Why this policy exists

3. This policy ensures that the Charity:

- Complies with data protection law, including the General Data Protection Regulation (UK GDPR) and follows good practice
- Protects the rights of guests, suppliers, business contacts, associates, employees, volunteers, Trustees of the Charity and other people the Charity has a relationship with or may need to contact
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data Protection Law

4. The General Data Protection Regulation (UK GDPR), describes how organisations must collect, handle, store and, where applicable share personal information.

5. These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

People, Risks and Responsibilities

Policy Scope

6. This policy applies to:

- Trustees, employees and associates of the Charity
- All contractors, suppliers, volunteers and other people working on behalf of Alma Beacon

7. It applies to all data that the Charity holds relating to identifiable individuals, even if that information technically falls outside of the General Data Protection Regulation. This data can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Personal data of guests, including potentially medical and/or criminal convictions
- Other information relating to individuals

Data Protection Risks

8. This policy helps to protect Alma Beacon from some very real data security risks, including:

- Breaches of confidentiality (for example, information being given out inappropriately)
- Failing to offer choice (for example, all individuals should be free to choose how the Charity uses data relating to them)
- Reputational damage (for example, the Charity could suffer if hackers successfully gained access to Special Category Data (previously sensitive data)

Responsibilities

Who is the Data Controller?

9. The Trustees of the Charity are the Data Controller for the purposes of the GDPR. They are ultimately responsible for ensuring that the Charity meets its legal obligations.

Security

10. Physical, electronic, administrative and managerial procedures have been introduced to safeguard and secure the information the Charity collects from individuals to protect their personal data against accidental, unlawful or unauthorised disclosure.

11. If an individual has any concerns about providing any data electronically, he/she can provide it by post. The Charity has implemented appropriate technical and organisational security measures designed to ensure that personal data remains private and secure.

12. Everyone who works for or with the Charity has responsibility for ensuring that personal data is collected, stored and handled appropriately.

13. Each team member that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles. However, the Trustees are responsible for:

- Approving any data protection statements attached to communications such as emails and letters
- Addressing any data protection queries from journalists or media outlets
- Where necessary, working with employees and volunteers to ensure any marketing initiatives abide by data protection principles
- Keeping themselves updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and related policies
- Arranging data protection training and advice
- Handling data protection questions from employees and volunteers
- Dealing with requests from individuals to see the data that the Charity holds about them (also called 'subject access requests')
- Checking and approving any contracts or agreements with third parties that may handle the charity's Special Category Data (previously known as sensitive data)
- Ensuring all systems, services and equipment used for storing data meet acceptable security standards
- Performing regular checks and scans to ensure security hardware and software is functioning properly
- Evaluating any third-party services, that the Charity is considering using to store or process data (for example, cloud computing services).
- Ensuring laptops and desktop computers have suitable passwords and are set to automatically switch into safe mode after a maximum of 20 minutes left idle

General employee guidelines

14. General guidelines applicable to all employees and Trustees of the Charity include:

- The only people able to access data covered by this policy should be those who need it for the work of the Charity
- Personal data should not be shared informally; when access to confidential information is required, employees can request it from a Trustee
- The Charity will provide training to any employees and volunteers to help them understand their responsibilities when handling personal data
- Employees and volunteers should keep all personal data secure, by taking sensible precautions and following the guidelines below
- In particular, strong passwords must be used, and they should not be shared

● Personal data should not be disclosed to unauthorised people, either within the Charity or externally

● personal data should be regularly reviewed and updated if it is found to be out of date; if no longer required, it should be deleted and securely disposed of

● Employees and volunteers should request help from the Trustees if they are unsure about any aspect of data protection

Data Storage

15. These rules describe how and where personal data should be safely stored. Questions about storing personal data safely can be directed to the Charity Secretary.

16. When personal data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

17. Where personal data that is usually stored electronically has been printed:

● The paper or files should be kept in a locked drawer or filing cabinet when not in use

● Employees and volunteers should make sure paper and printouts are not left where unauthorised people could see them, like on a printer

● Personal data printouts should be shredded and disposed of securely when no longer required.

18. When personal data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

● Personal data should be protected by strong passwords that are changed regularly and never shared between employees

● If personal data is stored on removable media (like a CD, memory stick or DVD), these should be kept locked away securely when not being used

● Personal data should only be stored on designated drives and servers and should only be uploaded to and approved cloud computing services

● Servers containing personal data should be sited in a secure location, away from general office space

● Personal data should be backed up frequently - those backups should be tested regularly, in line with the Charity's standard backup procedures

● Personal data should never be saved directly to laptops or other mobile devices like tablets or smart phones

● All servers and computers containing data should be protected by approved security software and a firewall

Data Use

19. Employees, volunteers and Trustees must ensure that, whenever personal data is accessed and used, the following requirements are observed:

- When working with personal data on screen, employees, volunteers and Trustees should ensure the screens of their computers are always locked when left unattended
- Personal data should not be shared informally and should never be sent by insecure email
- Personal data must be password protected before being transferred electronically
- Personal data must not be transferred outside of the European Economic Area without permission and unless the receiving body has demonstrated adequate safeguards
- Employees, volunteers and Trustees should not save copies of personal data to their own computers but should always access and update the central copy

Data Accuracy

20. The law requires the Charity to take reasonable steps to ensure that personal data is kept accurate and up to date.

21. The more important it is that the personal data is accurate, the greater the effort the Charity will take in order to ensure its accuracy.

22. It is the responsibility of all employees, volunteers and Trustees who work with personal data to take reasonable steps to ensure it is kept as accurate and up to date as possible, including the following:

- Personal data will be held in as few places as necessary; employees, volunteers and Trustees should not create any unnecessary additional data sets
- Employees, volunteers and Trustees should take every opportunity to ensure that personal data is updated
- The Charity will make it easy for data subjects to update the information held about them
- Personal data should be updated whenever inaccuracies are discovered

Subject Access Requests

23. All individuals who are the subject of personal data held by the Charity are entitled to:

- Ask what information the Charity holds about them and why
- Ask how to gain access to it
- Be informed how to keep it up to date
- Be informed how the Charity is meeting its data protection obligations

24. If an individual contacts the Charity requesting this information, this is called a subject access request.

25. Subject access requests from individuals will normally be made by e-mail to the Charity Secretary at secretary@almabeacon.org

26. The Secretary can supply a standard request form, although individuals do not have to use this.

27. The Data Controller must, under GDPR, supply the information within a maximum of one month.

28. The Data Controller will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing Data for Other Reasons

29. In certain circumstances, the General Data Protection Regulation allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

30. Under these circumstances, the Charity will disclose requested personal data. However, the Data Controller will ensure the request is legitimate, seeking assistance from legal advisers where necessary.

Providing Information

31. The Charity aims to ensure that individuals are aware that their personal data is being processed, and that they understand:

- How the personal data is being collected, stored used and shared
- How to exercise their rights

32. To these ends, the Charity has a Privacy Policy which explains how personal data is collected, stored, used and shared. It also sets out individuals' rights under the GDPR law, including the rights for access to what personal data is held by the Charity. This Privacy Policy is available on request and is on the Charity's website.

Updated: 15 July 2025: GH/JP