General Data Protection Regulation (GDPR) Policy

This policy applies to paid staff and volunteers of Winchester Action on Climate Change Ltd ("WinACC"). In this document, "volunteers" includes interns and other volunteers in the office, and also people who are active in action groups, at events and in other ways. It also applies to contractors, unless alternative arrangements have been agreed with them.

1. Introduction

The purpose of this policy is to enable WinACC to:

- comply with the law in respect of the data it holds about individuals;
- follow good practice
- protect WinACC's supporters, staff and other individuals
- protect WinACC from the consequences of a breach of its responsibilities

The GDPR gives individuals the right to know what information is held about them and also provides a framework to ensure that personal information is handled properly.

The GDPR defines who is a data 'controller' and who is a data 'processor'. In this case, WinACC is the data 'controller' and 3rd parties (such as Mailchimp or Gmail) are data 'processors'. All must comply with the principles of the Act, thus:

The GDPR works in two ways. Firstly, it states that anyone who processes personal information must comply with the following principles, in that the data must be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes subject

to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

And that the data controller (WinACC) must be "responsible for, and be able to demonstrate, compliance with the principles."

The second part of the GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

This policy applies to information relating to identifiable individuals. It includes all such information, regardless of whether it is held electronically or in paper form.

2. Definitions

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified, in particular by reference to an identifier (including name, identification number, location data or online identifier).

The data 'controller' determines the purposes and means of processing personal data.

A data 'processor' is responsible for processing personal data on behalf of a controller.

The 'data subject' is the individual whose personal data is being processed. Examples include: members, volunteers, WinACC News subscribers, donors, suppliers and staff (voluntary, prospective, current and past).

A 'personal data breach' is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

3. Policy Statement

WinACC will:

- comply with both the law and good practice
- respect individuals' rights

- be honest with individuals whose data is held
- provide training and support for staff and volunteers who handle personal data, so that they can act confidently and consistently.

WinACC recognises that its first priority under the GDPR is to seek consent from individuals to process their data. In this respect WinACC will:

- keep accurate information securely
- use it lawfully and for the purposes for which it was given.
- be open and transparent about the data held and how it is used.

4. Key Data Protection Risks

WinACC has identified the following potential key data protection risks, which this policy is designed to address:

- Breach of confidentiality (information being given out inappropriately)
- Breach of the GDPR itself
- Insufficient clarity about the range of uses to which data will be put, leading to Data Subjects being insufficiently informed
- Breach of security which makes information available to unauthorised people
- Failure to establish efficient systems of managing changes to contact details, leading to mailings not being sent to the correct recipients
- Insufficient clarity about the way personal data of people involved with WinACC is used, e.g. when it can be shared with other supporters to enable them to work together
- Inadequate wording in Data Processor contracts.

5. Responsibilities

The trustees recognise their overall responsibility for ensuring that WinACC complies with its legal obligations.

The Data Protection Officer is currently the Communications Manager, with the following responsibilities:

- Briefing the trustees on Data Protection responsibilities
- Reviewing Data Protection and related policies
- Advising staff, contractors and volunteers on Data Protection issues
- Ensuring that Data Protection induction and training takes place
- Handling access requests by Data Subjects
- Approving unusual or controversial disclosures of personal data
- Ensuring any contracts with Data Processors (e.g. WinACC's payroll provider) have appropriate data protection clauses that prevent data being used for any purposes other than to fulfil their contractual obligations to WinACC
- Ensuring adequate security measures are taken to protect personal data, whether held in physical or electronic form
- Approving data protection-related statements on publicity and other materials

All staff and volunteers are required to read, understand and follow any policies and procedures that relate to the personal data they may handle in the course of their work, including this policy and the Privacy Statement. Each WinACC Action Group will be asked to address data protection annually when the group's terms of reference and chairing arrangements are reviewed.

Significant breaches of this policy will be handled under WinACC's disciplinary procedures.

6. Confidentiality

Because confidentiality applies to a much wider range of information than Data Protection, WinACC has a separate Confidentiality Policy.

Where anyone within WinACC feels that it would be appropriate to disclose information in a way contrary to the Confidentiality Policy, or where an official disclosure request is received, this will only be done with the authorisation of the Data Protection Officer. All such disclosures will be documented.

7. Data Security

This section of the policy only addresses security issues relating to personal data. It does not cover security of other information, the building, business continuity or any other aspect of security.

WinACC has identified the following personal data security risks:

- Information passing between the office, staff, volunteers, contractors and third parties could go astray, be intercepted or be misdirected
- Staff or volunteers with access to personal information could misuse it
- IT security breaches could unintentionally give access to information about individuals
- Staff may be persuaded to give away information, either about supporters or colleagues, especially over the phone

Personal data held non-electronically (e.g. paper files) will normally be stored in the WinACC office which is locked to prevent unauthorised people gaining unsupervised access. If it is necessary to use this data off-site (e.g. by a home-worker), it will be transported with care and stored securely at its destination. Data will be destroyed securely when it is no longer required (and any retention period has expired).

Most personal data is held electronically in a small number of databases relating to contact details, mailing lists, website users and individual donors. Access to these databases is provided to office staff and volunteers as needed to run the charity efficiently. Recruitment and staff management procedures aim to ensure that people are sufficiently trustworthy for the roles assigned to them and that this trust is not abused.

Where appropriate, personal data kept electronically will be password-protected, for example if it is necessary to transfer lists of contact details to other computers (including by email) or to store them on computers to which non-authorised individuals might have access. Any memory sticks which are used to store or transfer personal data will be

password protected or encrypted. Secure back-up copies of information stored on WinACC's computers are made regularly.

When personal data has to be transmitted by post, appropriate precautions will be taken such as ensuring it is sent to the correct individual and where appropriate informing them that the data is on its way. It is never sent by fax.

Any breaches of data security will be investigated should they occur (see point 15).

8. Data Recording and Storage

WinACC reviews its procedures for ensuring that its records remain accurate and consistent at least once a year and, in particular:

- Data on any individual is held in as few places as necessary, and all staff and volunteers are instructed not to establish additional data sets.
- Effective procedures are in place so that all relevant systems are updated when information about any individual changes.
- Systems exist to ensure that data is corrected if shown to be inaccurate.

WinACC does not hold personal data for longer than it considers necessary. It has established retention periods for the following categories of data:

- Members – names and addresses will be held for at least ten years after membership ceases, as required by company law
- Website users – details provided on setting up a user account will be kept until the account is deleted
- Trustees – data required for the register of trustees will be held as required by company law
- Individual donors – details of donations will be kept for at least six years after the end of the relevant financial year
- Staff – personnel records will be kept for at least six years after employment ceases, and payroll data will be kept for at least six years after the end of the relevant tax year.
- Images - images (both moving and still images) will be retained for five years for people of 18 or over and three years for people under 18 because a person's image may change over time. If the image is to continue to be used, for instance on the website, social media or poster, re-consent for the image will be sought.
- Others not covered above (including volunteers and unsuccessful job applicants) – data which is no longer required will normally be deleted within one month, except for records required to ensure there is no accidental continuation of mailings which will be kept for no more than two years after a request to be removed from WinACC's mailings.

9. Data Subjects' Access to Data

Any requests by Data Subjects to see the information about them held by WinACC will be handled by the Data Protection Officer. WinACC aims to reply promptly and, in any case, within the legal maximum of 30 days.

Subject access requests must be made in writing, and there is no fee. All staff and volunteers are required to pass on any communication which might be a subject access request to the Data Protection Officer without delay. Where the person making a subject access request is not personally known to the Data Protection Officer their identity will be verified before handing over any information. The required information will be provided in permanent form unless the applicant makes a specific request to be given supervised access in person.

10. Transparency

WinACC is committed to ensuring that in principle Data Subjects are aware that their data is being processed and

- for what purpose it is being processed
- what types of disclosure are likely
- how to exercise their rights in relation to the data.

This GDPR policy is publicly available on our website. WinACC also has a Privacy Statement for Data Subjects, setting out how their information will be used, which is available on the WinACC website. Anyone who registers on the website is informed how we use their personal data when they register on the website. Staff will be informed about the use of their own personal data during their induction.

Whenever data is collected, the number of mandatory fields will be kept to a minimum. Data Subjects will be informed which fields are mandatory and, where this is not obvious, why.

11. Consent of Data Subjects

Consent is always sought for the processing of information about staff, and staff details will only be disclosed for purposes unrelated to their work for WinACC (e.g. financial references) with their consent.

Information about volunteers will be made public according to their role, and consent will be sought for (a) the means of contact they prefer to be made public, and (b) any publication of information which is not essential for their role.

Information about members and supporters will only be made public with their consent. This includes photographs. When joining WinACC, members have to consent to the addition of their name and address to WinACC's official register of members, which (in accordance with company law) must be available for public inspection at WinACC's office.

'Sensitive' personal data about members and supporters (including health information) will be held only with the knowledge and consent of the individual.

Consent will normally be sought in writing, although where this is not practicable (e.g. photographs) oral consent will be considered sufficient, subject to WinACC's specific policies in relation to the use of images of children and vulnerable adults. Attempts will be made at every opportunity to get consent in writing before the image is used.

All Data Subjects have to opt in to their data being used in prescribed ways and always have the opportunity to opt out.

WinACC acknowledges that, once given, consent can be withdrawn, but not this cannot apply retrospectively. There may be occasions where WinACC is required to retain data for a certain length of time, even though consent for using it has been withdrawn.

12. Direct Marketing

WinACC will treat the following direct communication with individuals as marketing:

- seeking donations and other financial support
- emails with footers advertising events
- WinACC News
- promoting any paid-for WinACC events and services
- promoting membership to supporters;
- promoting sponsored events and other fundraising exercises
-

Individuals can opt-out of marketing communications at any time by contacting the WinACC office, or by 'unsubscribing' on emails, weblinks or other communications.

13. Mailing Lists

WinACC will not share its mailing lists (or carry out joint or reciprocal mailings) with third parties unless WinACC is working in partnership with the third party for a purpose for which the Data Subject gave their information to WinACC – for example, to inform them of a jointly hosted meeting.

Data given to WinACC for the purposes of specific projects may be used by WinACC for other activities which have similar aims but will not be used for other types of WinACC activity.

WinACC undertakes to obtain external mailing lists only where it believes that the list is up-to-date and from an organisation with appropriate data protection measures. For example, it might use parish councillor contact details provided by Winchester City Council.

All WinACC materials asking people to give contact details (including email address or telephone or full mailing address or social media details) will reflect the principles of the GDPR.

14. Staff training and Acceptance of Responsibilities

The content of this Policy and the Privacy Statement will be described briefly in the induction of anyone who works or volunteers in the WinACC office. All staff and office volunteers who have access to any kind of personal data will have their responsibilities outlined during their induction.

WinACC encourages its staff and volunteers to seek guidance from the Data Protection Officer if they are unclear about any of their Data Protection responsibilities or to request training.

15. Breach

In the event of a personal data breach WinACC will establish the likelihood and severity of the resulting risk to the data subject's rights and freedoms. If WinACC considers that it is likely that there will be a risk then WinACC will notify the Information Commissioner's Office

within 72 hours of becoming aware of the breach. If WinACC considers it is likely that there will be a high risk, WinACC will also inform the data subject as soon as possible. If WinACC considers that a risk is unlikely, it will record this decision in writing.

WinACC will also review the circumstances which led to the personal data breach and take steps to seek to minimise the risk of such a breach occurring in the future.

16. Breach

This policy is intended to be reviewed at least annually to take account of any changes in relevant legislation, contractual arrangements, good practice or in response to an identified failing in its effectiveness.

Version control

Date	Issue	Status	Description
May 2018	1	Approved by WinACC's trustees	This policy was first approved following the UK's new Data Protection Act (2018).
June 2020	2	Approved by WinACC's trustees	
10 August 2022	3	Approved by WinACC's trustees	