ACE Newburgh Data Protection Policy

Purpose and Scope: This Data Protection Policy sets out how ACE Newburgh handles personal data and ensures compliance with data protection laws. It is intended for internal use by our trustees and volunteers (especially those handling personal information), but it is also available publicly to demonstrate our commitment to good practice. The policy covers all personal data processed by ACE Newburgh relating to individuals, including volunteers, members, donors, trustees, and any other contacts. By following this policy, we aim to protect individuals' privacy and our organisation's integrity.

Our Commitment: ACE Newburgh will manage personal data lawfully, fairly, and transparently. We adhere to the core **data protection principles** established by the UK GDPR. In practice, this means:

- **Lawfulness, Fairness, Transparency:** We will only collect and use personal data in ways that are legally permitted, and that people would reasonably expect. We will be open and clear about what data we collect and why (through privacy notices like our Privacy Policy).
- **Purpose Limitation:** We collect data for specific, legitimate purposes related to our charity's aims (such as coordinating volunteers, managing memberships, and complying with our legal obligations). We will not use the data for completely unrelated purposes without obtaining consent or having a clear lawful justification.
- **Data Minimisation:** We only ask for and keep the minimum personal information necessary for the task at hand. If data is not needed, we won't collect it. For example, we may need contact details to reach volunteers, but we won't ask for irrelevant details like national insurance numbers or bank details unless absolutely required (e.g. if you become an employee or need an expense reimbursement, then bank info is used just for that transaction).
- **Accuracy:** We will keep personal data accurate and up to date. We rely on individuals to inform us of changes (like a new email address), and we will promptly update our records when we're notified. Periodically, we may verify information (for instance, asking members to confirm their contact details annually).
- **Storage Limitation:** We will not keep personal data longer than necessary. Our retention practices (detailed in the Privacy Policy and internal guidelines) ensure we delete or anonymise data that is no longer required for the purpose it was collected, unless law requires a longer retention.
- **Integrity and Confidentiality:** We protect personal data with appropriate security measures (technical and organizational) to prevent unauthorised access, loss, or damage. This includes using passwords on files, limiting access, and awareness training for those handling data.
- **Accountability:** ACE Newburgh's trustees understand that we are responsible for complying with data protection principles and must be able to

demonstrate this compliance. All trustees and any volunteers handling data are expected to adhere to this policy and support its implementation.

Roles and Responsibilities: Because ACE Newburgh is a small organization without paid staff, our Board of Trustees collectively acts as the data controller. However, for practical purposes, we designate a lead trustee for data protection (Data Protection Lead) to coordinate compliance efforts. Key responsibilities include:

- Ensuring that privacy notices (like the public Privacy Policy) are kept up to date and reflect our practices.
- Keeping an inventory of what personal data we hold and how it is used (even a simple list of datasets: e.g. “Member list, Volunteer contact list, etc.”).
- Handling any data protection queries or requests from individuals (such as subject access requests) in a timely manner.
- Making sure that all trustees and relevant volunteers are aware of this policy and have basic training on data protection principles.
- Monitoring compliance and advising the Board on any data protection risks or issues. For example, if we plan a new project involving personal data (like collecting survey responses from residents), considering data protection at the planning stage (this is sometimes called “privacy by design”).
- Keeping this policy under review and proposing updates as needed.

All Trustees, and any volunteer who handles personal information, must:

- Familiarise themselves with this Data Protection Policy and the related Privacy Policy.
- Only collect and access personal data as needed for their role.
- Keep data secure (e.g., not share passwords, not download data to unsecured personal devices, etc. unless with proper safeguards).
- Report any potential data breaches or losses immediately to the Data Protection Lead (so we can take action to mitigate and notify if required).
- When in doubt, seek guidance – e.g., if someone isn’t sure whether they can share a member’s contact info with another member, or if they receive an unusual request for data, they should check with the Data Protection Lead or Chair.

Collecting Personal Data: When collecting personal data (through forms, sign-ups, etc.), we will provide a clear explanation (privacy notice) of why we need it and how it will be used, if not obvious. For example, our volunteer application form will state that the information will be used to contact the volunteer and match them with suitable opportunities. We will avoid collecting more data than we need. If we ever collect data on children (under 16) in a context that requires parental consent, we will ensure consent is obtained from a parent/guardian in line with legal requirements.

Using and Sharing Personal Data: Personal data should only be used for the agreed purpose. ACE Newburgh trustees/volunteers should **not** use data entrusted to us for their personal or any unauthorised purposes. For instance, having access to the volunteer email list does not mean a trustee can email them about unrelated causes or share that list with another group. Any sharing of data with third parties must be approved by the Board (or the Data Protection Lead on behalf of the Board)

and must be covered by a proper agreement or assurance that the third party will handle the data legally and securely. As noted in our Privacy Policy, routine sharing is very limited (mainly within the team, or to service providers like an email service). If uncertain, treat the data as confidential and **do not disclose it** until permission or advice is obtained.

Data Security Measures: We employ several practical security measures:

- **Access Control:** Personal data files (e.g. membership lists) are accessible only to those who need them. If stored on cloud services or collaboration tools, access permissions are restricted. We also use administrative protections like not keeping data on public computers.
- **Passwords and Encryption:** Sensitive files are password-protected. Devices used by trustees for ACE Newburgh work (personal laptops, etc.) should have secure logins. If highly sensitive data were held (none currently), we would use encryption or specialised secure storage.
- **Avoiding Data Breach Risks:** We avoid using insecure channels for personal data. For example, we wouldn't ask volunteers to send sensitive info via an open social media page. When sending group emails, we use blind-copy (BCC) for group emails to volunteers/members to avoid exposing addresses. We also refrain from unnecessarily printing personal details; any papers used (e.g. sign-in sheets) are collected and stored or disposed of securely.
- **Website and Online Services:** We maintain our website and any online tools with security updates and best practices to prevent hacking or data leaks. (Currently, since we do not collect personal data through the website, the risk is low, but we remain vigilant).
- **Incident Response:** In the event of a **data breach** – for example, if a laptop with member data is lost or if we mistakenly email personal details to the wrong recipient – the person who discovers it must inform the Data Protection Lead immediately. We will assess the breach, take steps to contain it, and inform affected individuals without undue delay if there is a risk to them. We are also aware of the legal requirement to report certain serious breaches to the ICO within 72 hours, and the Data Protection Lead will handle such reporting if criteria are met.

Individual Rights and Requests: All trustees/volunteers should be aware that people can exercise their data protection rights (as listed in the Privacy Policy: access, rectification, erasure, etc.). If any trustee or volunteer receives a communication from someone about their data – for example, a volunteer asks, "What information do you hold on me?" or a member says "Please delete my data" – you should forward that request to the Data Protection Lead **immediately**. We have a responsibility to respond to such requests, typically within one month. The Data Protection Lead will coordinate the response but may need cooperation (e.g. gathering data from various files). We do not charge a fee for handling requests, except in the rare case of excessive or repeated requests as allowed by law (even then, we aim to handle requests without cost).

We will honour objections to marketing or general communications – for instance, if someone opts out of newsletters, everyone involved in communication must ensure that preference is respected.

Data Protection Impact Assessments (DPIA): Given our small size and low-risk use of data, formal DPIAs will seldom be required. However, if we embark on a new project that involves handling personal data in a way that could be high-risk (for example, collecting health information for a community support project, or using new technology to process data), we will carry out a proportionate risk assessment. Essentially, we'll ask: "What are the privacy risks and how can we reduce them?" and document the answers. The Data Protection Lead will oversee this process and consult guidance or the ICO's DPIA templates as needed.

Third-Party Processors: If we use third-party services (like cloud storage, email distribution software, survey tools), we will:

- Choose providers that are reputable and preferably have data servers in the UK or EU (or certified under schemes like UK "adequacy" or EU Standard Contractual Clauses for international transfers).
- Establish a proper agreement or accept terms that align with data protection requirements – ensuring they only use the data for our purposes and protect it.
- Only give them the data that's needed for the service. For example, if using an email newsletter service, we upload the name and email of subscribers, not other details.

Confidentiality and Volunteer Conduct: Anyone handling personal data for ACE Newburgh is expected to keep that information confidential and secure. Even within the organisation, do not freely discuss personal details without good reason. For example, trustees might discuss how to engage volunteers generally, but shouldn't gossip about an individual volunteer's personal circumstances. A simple rule: treat others' personal information as you'd want yours to be treated.

Consequences of Policy Breach: While we are all volunteers, data protection is a serious matter. A breach could harm individuals in our community and damage trust in our charity. Significant negligence or willful disregard for this policy by a trustee or volunteer could result in the Board taking appropriate action, such as removal from a role or referral to authorities if laws were broken. Our approach is supportive – we prefer to educate and prevent issues – but we cannot ignore serious mishandling of personal data.

Policy Review: This Data Protection Policy will be reviewed **annually** alongside the Privacy Policy. Updates will be made as needed, for example if laws change or if we start new activities that impact data protection. All trustees will approve the policy and any revisions. New trustees or volunteers who take on data-related tasks will be given a copy of this policy and an overview of its importance during induction.

By following this policy, ACE Newburgh ensures it respects the privacy of our community and maintains the trust placed in us as guardians of personal information.

Data protection is not just a legal duty but part of operating ethically and transparently in our community.

Last updated: 01November 2025