The Mary Tavy Jubilee Group

Data Protection Policy

Mary Tavy Jubilee Group [the Group] will do all that is required to comply with the General Data Protection Regulations.

The GDPR are underpinned by six principles. Each person handing personal data on behalf of the Group must at all times comply with all of these principles:

1. **Fair, lawful and transparent**

   We will only use personal data for lawful reasons and ensure we are transparent about the way that we process personal data.

2. **Purpose limitation**

   We will only use personal data for the purposes originally intended.

3. **Data minimisation**

   We will limit processing of personal data to the minimum necessary to perform the intended task.

4. **Data accuracy**

   We will ensure that any personal data we use is accurate and where necessary kept up-to-date.

5. **Data retention**

   We will not hold personal data for any longer than is necessary.

6. **Data security**

   We will make sure that we keep personal data secure.

Personal data

Personal data is any data that relates to an identifiable individual, such as name, address, contact details, age or gender. It also includes photographs of identifiable people.

Certain categories of personal data are subject to strict rules regarding collection and processing, such as racial or ethnic origin, health and medical information and sexual orientation. Mary Tavy Jubilee Group will at no time ask for or hold such information.

Obtaining consent

We will obtain consent before adding any personal data to the Jubilee News distribution list, event lists or other lists required to administer the Group. Such consent may be by email, written down, or by way of any forms issued, but may not be oral. If processing personal data about children under 13 we will need to obtain parental consent.

Data Controllers and Data Protection Officer

Trustees and any other officers or post holders may need to handle data and are therefore Data Controllers. The Trustees will appoint a Data Protection Officer [DPO] to monitor compliance and to ensure that Data Controllers are aware of the requirements of the Regulations.

The DPO will ensure that this policy document is regularly reviewed and updated as necessary, at least once a year.

Mary Tavy Jubilee Group is exempt from the requirement to notify the ICO (Information Commissioner's Office) that personal data is being processed.

Lawful purposes

The lawful purposes for which the company may hold and process data are: production and distribution of Jubilee News, general contact lists, event management and booking, general enquiries, trustee data, accounts.

Securely held

Any lists held on a computer will be password protected. Only the individual Data Controllers and the Data Protection Officer are to know the password.

The rights of individuals

Individuals may obtain confirmation from the DPO as to whether or not personal data concerning them is being used, where and for what purpose. A copy of the personal data will be provided on request, free of charge, in an electronic format, including any emails where they are mentioned. If the data was not obtained from the individual, details of where it came from will be provided. This is called a Subject Access Request [SAR]. It may be that the DPO will need to verify the individual's identity otherwise a data breach could result. The DPO has 30 days in which to respond.

There are exceptions to this right, such as if the request is 'manifestly unfounded or excessive'.

Individuals also have the right to have data rectified if incorrect or incomplete and to have data erased where there is no compelling reason for it to continue to be held.

Data breaches

A data breach is when personal data is passed on, stolen or hacked, and risk to individuals may result. The data may have been on a computer, CD or memory stick, mobile phone or on paper.

Data Controllers are required to report data breaches to the DPO, and certain types of data breach need to be reported to the Information Commissioner's Office [ICO], and in some cases to the individuals affected. A report to the ICO must be made within 72 hours (3 days) of the company becoming aware that an incident is reportable.