Executive Summary

The General Data Protection Regulations (GDPR) came into force from 25th of May 2018 and is mandatory for any organisation holding personal data about individuals, regardless of the size of the organisation.

Statement of Limitation of Liability

This document has been prepared on a best endeavours basis and is presented as our understanding of the GDPR law as it is applicable to the Friends of Marble Hill (the Friends). It is published on the Friends website.

Key issues

The Friends stores a minimum amount of personal data

- Email address of the member, in effect the Membership ID
- First name associated with the email address
- Last name associated with the email address

This data held by the Friends is used for the following:

- Members who are identified as part of the Friends and who pay a subscription fee and receive benefits and newsletter
- Members who have purchased tickets for events arranged by the Friends
- Members who receive marketing information about forthcoming events

Communication

For email communication to facilitate those objectives, the Friends use the following email address: friends@friendsofmarblehill.org.uk

Except for the email list of members, the primary lawful basis of communicating with others via email is for the performance of a contract (i.e. being a membership organisation, we might provide events to our members, arranging contracts which do not necessarily need to be financial). This might include communicating by email with contractors, guest speakers for events, organisers of events etc. It might also include communication via email with the general public to respond to enquiries etc. In these circumstances the information will NOT be stored in a database, but will be held in the email system using the above mentioned email address.

For questions about membership, email: membership@friendsofmarblehill.org.uk

For questions about your subscription, email: treasurer@friendsofmarblehill.org.uk

Table of Contents of this GDPR policy

Overview of GDPR

GDPR Principles

Lawful Processing

Consent

Performance of a Contract

The Friends GDPR Policy and Compliance Statement

Securing Individuals' Data

Data held with respect to Friends meetings

Highly Sensitive Data

Individual Rights

Subject Access Requests

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

The right to data portability

The right to object

Rights in relation to automated decision making and profiling

Accountability

Managing a Data Breach

Registration

Training

Privacy Notice and Policy

This GDPR policy, and Privacy notice and policy has been prepared by and approved by the Committee of the Friends of Marble Hill.

A copy can be found on https://friendsofmarblehill.org.uk

For and behalf of The Friends

March 2022

Overview of GDPR

The General Data Protection Regulations came into force from 25 May 2018 are regulations that are law. They were introduced by the European Union as a way of standardising storage and processing of personal information and protecting individuals' data and modernisation of the Data Protection Act (1998). Even though the UK is no longer a member of the EU the GDPR is the law in the UK.

GDPR Principles

GDPR is about personal data. Personal data is information that can be connected to a member.

The Friends is both a "controller" and a "processor" of personal data.

Controller: Controls the personal data; acquisition, quality, storage and disposal.

Processor: Manipulates data to do things such as sending emails, invoices, newsletters.

In the Friends the "controllers" are the Membership Secretary and the Treasurer who have access to the personal information about members. This includes the first name and last name associated with an email address necessary to communicate with members and to reconcile subscriptions received from members into the Friends bank account.

Certain 'special categories of data' can only be stored with explicit consent (or certain statutory reasons for exception). For the avoidance of any doubt the Friends do NOT maintain any of the following information: racial or ethnic origin, political opinions, religious beliefs, sexual preferences or health data about its members and so do NOT need to give special consideration to obtaining and recording consent.

The GDPR requires that the Friends demonstrates how it is complying with the law and, as a result, explicit policies have been written down and signed off by the Committee of the Friends.

To clarify, information about individuals in the public domain is not affected by these rules. This includes for example a newsletter article which names members of the Committee, or those involved in furthering the vision and purpose of the Friends and or those named on the Friends' website.

Lawful Processing

Processing personal data must be within the law and several options for justifying this are allowed – the most relevant (a full list is in GDPR Articles 6 and 9) to small organisations are:

6(1)(a) – Consent of the data subject

6(1)(b) – Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract

Consent

Consent under GDPR must be freely given, specific, uninformed and an unambiguous indication of the individual's wishes. There must be a positive opt-in and consent cannot be implied from silence, pre-ticked boxes or inactivity.

Consent must be separate from other terms and conditions and the must be simple ways to withdraw consent. Consent must be verifiable.

Performance of a Contract

Processing for the performance of a contract is an important principle - if an individual wishes to become a member of the Friends - then for the Friends to function and provide the services to the member, records must be kept and so there is no need to obtain explicit additional consent for the storage of that information.

Consent is required to share information with third parties such as other clubs or a national organisation i.e. English Heritage.

The Friends has a minimum age of 18 to be a member. So, for the avoidance of doubt, the Friends does NOT offer any services to and or store data about children (defined as under the age of 16). As a result the Friends will NOT require any person holding any parental responsibility to give any consent to become a member.

The Friends recognise that an application for membership could be submitted by someone less than 18. In order to become a member it will be necessary for a subscription fee to be paid via a bank transfer. The minimum age for having sole control over a bank account is 16. The Friends consider the risk to be minimal that those aged less than 18 will apply to become members and pay for a subscription.

The Friends GDPR Policy and Compliance Statement

This outlines GDPR responsibilities and how the Friends meet those requirements.

GDPR requires that:

> *Article 5 – The controller shall be responsible for, and be able to demonstrate, compliance with the principles.*
>
> *(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;*

Information collected and the legal basis for it is identified in the Friends Privacy notice.

> *(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;*

Processes for individuals to view and correct their personal data held by Friends in the Friends Privacy Notice

> *(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;*

The terms of data storage are for no longer than six years for information about contractors, customers and members and two years for any email marketing communication in order to meet the requirements in the event of a tax audit by HMRC and data will be destroyed after this.

> *(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*

Personally identifiable data will be handled with care and consideration in line with GDPR by all committee members, and third parties who come into contact with it. Data is secured and used only in line with its agreed purposes.

In the event of a data breach the Friends committee will investigate the causes, inform individuals affected and provide them with appropriate information and actively seek to prevent further occurrences in the future.

Securing Individuals' Data

The Friends data is secured safely in a way that the information can't be accessed by unauthorised individuals or shared by accident.

The Friends information is stored securely, but due to minimum amount of information stored, the Friends do NOT provide any online access to a member.

Any request to change a first name or last name associated with an email account to arranged by a member sending a request to the Friends via email.

The only email address used to communicate between the Friends and members is: friends@friendsofmarblehill.org.uk

The Friends will protect the email addresses of its members by either sending out an individually addressed email or by "BCC" (Blind Carbon Copy).

The Friends will NOT share the email addresses of its members.

The Friends ensures security by restricting access to lists of email addresses to trusted responsible members of the Friends and by emphasising a culture of not sharing email addresses inappropriately.

This is achieved by using a mailing list service that sends out the emails individually on the organisation's behalf (for example using MailChimp).

In certain situations when a member or others email the Friends, then a response will be forthcoming directly from the Friends email address.

Data held with respect to Friends meetings

There are three types of meetings:

1. Annual General Meeting (AGM)
2. Extraordinary General Meeting (EGM)
3. Committee meetings

The AGM and EGM are not recorded. Once the Chair has determined that a quorum has been formed to hold the meeting, it is only the members of the Committee / their roles in the Committee that are recorded in the minutes of the meetings.

Other names of members of the Friends are not recorded in published minutes unless there has been prior consent given by the member.

Committee meetings are not recorded. The only record of the meetings are the minutes approved by the Committee. It is the practice of the Committee NOT to mention any specific names of individuals unless they are a member of the Committee and or have given their approval.

Highly Sensitive Data

The Friends is of the opinion it does NOT manage highly sensitive data, such as Disclosure and Barring Service (DBS) reports or health records.

Individual Rights

GDPR gives individuals i.e. the members of the Friends the following rights:

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.

Subject Access Requests

This covers:

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

The right to be informed

A key part of GDPR is that a member can request to see copies of all the information that the Friends holds about them.

The Friends only directly holds the following information about a member:

- Email address of the member - in effect the Membership ID
- First name associated with the email address
- Last name associated with the email address

At anytime a member can make a request to obtain the first name and last name associated with an email address.

The Friends will only accept an email from the membership ID email address. The Friends will only reply to that membership ID email address.

The right of access

On a Subject Access Request to the membership secretary sent from the email address of the member a copy of the membership records for the individual containing the first name and last name of the member will be provided as well as any information stored on MailChimp.com on behalf of Friends.

Additionally, on request, a search of and list of emails that have been retained to or from the individual to the other Friends email addresses will be provided.

On a specific request, a record of the payment of subscriptions identified by the Friends will be provided. The Friends do not maintain any information about the source of the funds of subscriptions and so cannot provide the name of the originating bank, sort code or account number or account name.

For the avoidance of doubt the Friends do NOT maintain any paper data relating to the member.

All information will be provided free of charge and will usually be completed within two months. If the Friends anticipate a delay in providing the information the member will be contacted within forty five days of submitting the request.

The right to rectification

If information about a first name or last name is incomplete or incorrect then it will be corrected by the membership secretary within one month.

The right to erasure

Information about individuals will be deleted as far as possible on request except where it may be required for tax purposes in which case it will be deleted six years after it was obtained or last name used. Information for marketing purposes will be deleted two years after it was last name used or upon request.

The right to object and to restrict processing

Due to the nature of the activities undertaken by the Friends, the Friends are of the opinion that members have no cause to request a restriction in processing of the members' data.

The reason being that if an individual wishes to become a member of the Friends - then for the Friends to function and provide the services to the member, records must be kept and so a) there is no need to obtain explicit additional consent for the storage of that information and b) it is implicit the information (email address and name) will be used when providing the member with member services and benefits.

However, if a member considers that their rights under the GDPR are being contravened then they have the right to email the membership secretary outlining their concerns which will be reviewed by the committee and responded to. In such instance the member is requested to highlight any concerns by reference to specific clauses within the Constitution which is available on the Friends website to which the member agreed when becoming a member.

The right to data portability

Upon request, the membership secretary will provide a copy of the membership information and ticket sales information relating to an individual in electronic format. This will be completed within two months.

The right to object

A member can email the Friends via the membership secretary to terminate their membership at any time. This will result in them no longer receiving any of the benefits of membership.

Rights in relation to automated decision making and profiling

The Friends does not use any automated decision-making or profiling technologies. Communications with members are with all members.

Accountability

There is a requirement that the controller is responsible for complying with the GDPR and demonstrating that they have done so.

The Friends demonstrates compliance by:

- Limiting the access to data to only authorised members / officers of the Committee and / or those specifically delegated by the Committee to process the data in order to communicate via email.
- Measures that meet the principles of data protection including data minimisation, transparency, and having a secure process to maintain the membership register.

Privacy By Design has long been a principle that organisations are required to follow. The Friends follow this principle by storing only information that is relevant and not excessive.

Managing a Data Breach

A personal data breach is where a lapse in security results in accidental or unlawful destruction alteration disclosure or access to personal data maintained by the Friends.

Certain categories of data breach such as those which "*result in a high risk of adversely affecting individual's rights and freedoms*" must be reported to the Information Commissioner's Office (ICO).

The Friends, by keeping the least possible information about members are of the view that any data breach is unlikely to reach this threshold (i.e. the accidental loss of an individual's name and email and membership status is unlikely to have significant impact on the individual although it may annoy them).

The Friends have a process in place to identify and manage data breaches that might include:

- Accidental sharing of information by the Friends members including members of the Committee
- Malicious sharing of information by the Friends Committee members
- Hacking and theft by third parties

That process is the summoning of an emergency Committee meeting by any member of the Committee who has any concern about a data breach and or knowledge of a data breach. The Committee meeting will be held within one week.

.

Registration

It is a legal requirement to be registered with the Information Commissioner's Office (ICO) and pay a fee unless the organisation meets an exemption criteria. One of these criteria is to be a not-for-profit organisation, providing all three apply:

- "*you are only processing data for the purposes of establishing or maintaining membership or support for a body or association not established or conducted for profit, or providing or administering activities for individuals who are members of the body or association or have regular contact with it*
- *you only hold information about individuals whose data you need to process for this exempt purpose*
- *The personal data you process is restricted to personal information that is necessary for this exempt purpose*"

The Friends fulfil that exemption criteria and for that reason the Friends is not registered with the ICO.

Training

All members of the Committee are required to certify annually (before each AGM) to the Chair that they have read this GDPR document.

It is a requirement that all new members of the Committee are required to certify to the Chair that they have read this GDPR document.

Once per year a member of the committee will be dedicated to:

- reviewing the principles of GDPR compliance
- reviewing changes to the organisation and its processes and whether this has an impact on data protection and GDPR
- assess and provide the necessary training needs associated with protecting and managing individuals' data in line with GDPR requirements.

Commencing in the financial year 1 April 2022 – 31 March 2023 this review will be conducted by 30th June each year with a report submitted to the first Committee meeting after 30th June.

Additional training will be provided on request for any member of the Committee who needs it.

Privacy Notice and Policy

Summary of the key points:

GDPR Requirements	**Friends of Marble Hill Policy**
Purpose of the processing and the lawful basis for the processing	Information is stored to enable the Friends to provide membership services and/or tickets to our shows.
The legitimate interests of the controller or third party, where applicable	(n/a)
Any recipient or categories of recipients of the personal data	Information is not be shared with third parties although we use MailChimp.com as data processors to provide services for members.
Details of transfers to third country and safeguards	MailChimp complies with GDPR regulations and other data processing rules.
Retention period or criteria used to determine the retention period	Information about members and customers is retained for a maximum of six years (in line with HMRC tax law) after the last name contact with us. Information about email list subscribers will be deleted after two years of inaction/no contact.
The existence of each of data subject's rights: • *The right to be informed* • *The right of access* • *The right to rectification* • *The right to erasure* • *The right to restrict processing* • *The right to data portability* • *The right to object* • *Rights in relation to automated decision making and profiling.*	A members' rights under the GDPR are not affected and a member has the right to view their data, correct any error or ask for it to be erased. A member can ask for a report showing the first name and last name associated with the member's email address at any time.

The right to withdraw consent at any time, where relevant	A member can cancel their membership at any time.
The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences.	The Friends does not use any automated decision-making or profiling technologies. Communications with members are with all members.
Identity and contact details of the controller (and where applicable, the controller's representative) and the data protection officer	Information is managed by the membership secretary who can be contacted at membership@friendsofmarblehill.org.uk treasurer@friendsofmarblehill.org.uk
The right to lodge a complaint with a supervisory authority	If a member wishes to complain about the handling of your personal data can make a complaint to the information Commissioner's office (www.ico.org.uk)
Whether the provision of personal data part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data	If a member chooses not to provide personal information for us to process, the Friends will be unable to provide membership services, register an individual for events or send emails about upcoming events.

Friends of Marble Hill - Privacy Policy

The Friends have a Privacy Policy that applies to all members and is available on its website and explains how the Friends comply with GDPR.

Who are we?

We are the Friends of Marble Hill:

Our website address is: https://friendsofmarblehill.org.uk

Our Vision:

- The secured future of Marble Hill House and Park as a valued community asset.

Our Purpose

- Connect the local community with English Heritage so that Marble Hill is valued and protected for the benefit of all users.
- Provide a communication channel for users of Marble Hill independently of English Heritage.

How do we comply with GDPR?

The Committee of the Friends has assessed the GDPR as it relates to the Friends. This document setting out compliance with GDPR is available on the Friends website at ……

In summary, personal details will be stored and processed in accordance with the General Data Protection Regulations. Further information on this and your rights is available in this Privacy Policy available on the Friends website at ……

Information will be used to provide you with membership and / or ticket services and will not be shared with third parties.

What personal data we collect and why we collect it?

We collect three pieces of personal data:

1. Email address of the member - in effect the Membership ID
2. First name associated with the email address
3. Last name associated with the email address

This data held by the Friends is used for the following:

- Members who are identified as part of the Friends and who pay a subscription. fee and receive benefits and newsletter.
- Members who have purchased tickets for events arranged by the Friends.
- Members who receive marketing information about forthcoming events.

What rights you have over your data?

If you are a member, you can request to receive an email with the first name and last name associated with the email address. You can also request that we erase any personal data we hold about you by stopping your membership. This does not include any data we are obliged to keep for administrative, legal, or security purposes including retaining details of a former member for the purposes of reconciling the financial statements of the Friends until such time that information is no longer required.

If you have any questions about your membership please contact the membership secretary at membership@friendsofmarblehill.org.uk

If you have any questions about your subscription please contact the Treasurer at treasurer@friendsofmarblehill.org.uk

What automated decision making and/or profiling we do with user data?

The Friends does not use any automated decision-making or profiling technologies. Communications with members are with all members.

Where we send to or with whom do we share your data?

We do not send your data to anyone and do not share or sell your data.

We though use MailChimp.com as data processors to provide services for you.

- MailChimp.com: The Friends use this service to manage its communication with members making it easy to control storage of personal data, allow recipients to unsubscribe and comply with GDPR.

What data breach procedures we have in place?

The Friends have a process in place to identify and manage data breaches that might include:

- Accidental sharing of information by the Friends members including members of the Committee
- Malicious sharing of information by the Friends Committee members

- Hacking and theft by third parties

That process is the summoning of an emergency meeting of the Committee to be held within 48 hours by any member of the Committee who has any concern about a data breach and or knowledge of a data breach.

Embedded content from other websites

Articles on the Friends website may include embedded content (e.g. videos, images, articles, etc.). Embedded content from other websites behaves in the exact same way as if the visitor has visited the other website.

These websites may collect data about you, use cookies, embed additional third-party tracking, and monitor your interaction with that embedded content, including tracking your interaction with the embedded content if you have an account and are logged in to that website. The Friends will not accept any responsibility for the viewing and or use of the Friends website and or any other links to other websites.

END