Data Protection Policy

Friends of the Black Watch Castle and Museum - SC 041823

1 Definitions

Data Controller - the controller says how and why personal data is processed

Data Processor - the processor acts on the controller's behalf

Data Subject - the individual to whom the data relates

Right to hold data - one can rely on other lawful basis apart from consent where processing is necessary for the purposes of the Friends of the Black Watch Castle and Museum (Friends) legitimate interests.

The definition of Personal Data is:

Information which relates to a living individual identified:

- from that data
- from that data and other information which is or is likely to be in the possession of the Data Controller
- held electronically or manually in a relevant indexed filing system

e.g. Name, job title, telephone number, email address, date of birth, postal address.

Particular care must be used when handling Sensitive Personal Data which may be defined as:

- defining racial or ethnic origin
- political opinions
- religious or similar beliefs
- trade union details
- health data
- sexual orientation data
- offences or alleged offences (removed in General Data Protection Regulation, GDPR, after 28th May 2018)
- court proceedings (removed in GDPR after 28th May 2018)
- biometric or genetic data (added in GDPR after 28th May 2018)

All the above Sensitive Personal Data falls outside of our requirements therefore should not be held.

2 Introduction

Data Protection Act (DPA) was passed by Parliament in 1998. The General Data Protection Regulations (GDPR) becomes law on 28 May 2018. This policy is designed to be applicable under both sets of legislation.

The basic principles of Data Protection are that personal details are the property of the individual and we may only hold information and use it in the way that the individual allows us to and relevant to the operation of the Friends. There are four fundamental conditions under which we hold personal data. They are:

1. We only hold data which is relevant to the purposes and services of the Friends
2. The data we hold must be accurate and up-to-date

3. Any data not relevant or no longer required is deleted both from current storage and back-up
4. The data must be kept secure and only those officers, volunteers, Black Watch Castle and Museum (Museum) staff, system administrators and third party operators that require access as part of their function may be allowed access to the data

Furthermore, anyone on whom we hold data is entitled to see any data we hold on them and can require any errors to be corrected. Any data so corrected must be passed on to third parties to whom the data has previously been supplied.

Processing is handling data in any way:

- collecting personal data
- storing in a database
- ordering in a filing system
- editing data records
- transmission onwards to a third party

So the Friends fall within the definition of both data controllers and data processors.

Privacy breaches can lead to limitless financial penalties, bad press, damaged reputation, loss of trust from supporters and loss of revenue. It is in all of our interest to handle data appropriately. Data privacy is relevant to – and the responsibility of – everyone in the Friends.

3 Data Protection Register

Self-assessment as to the need to register under the Data Protection Act was undertaken with the result that there was no requirement to register as the organisation is exempt. Data entered was as follows:

Do you use CCTV for the purposes of crime prevention? – No

Are you processing personal information? – Yes

Do you process the information electronically? – Yes

Is your organisation responsible for deciding how the information is processed? – Yes

Do you only process information for judicial functions, domestic or recreational reasons or to maintain a public register? – No

Are you a not-for-profit organisation that qualifies for an exemption? – Yes

4 Minimum Requirements

1 **We must tell people what we are doing with their data**

People should know what we are doing with their information and who it will be shared with. This is a legal requirement (as well as established best practice) so it is important we are open and honest with people about how their data will be used. To this end a privacy statement is to be published on the website and in membership welcome/renewal letters. The privacy statement as follows: “Personal data provided by a Member to the Friends of the Black Watch Castle and Museum will be used solely for the purpose of communicating with the Member about events relevant to the membership and matters related to the organisation of the Friends of the Black Watch Castle and Museum. It will not be passed to any third party for any other purpose unless this is required by law”.

2 **Make sure all people with access to the data are adequately trained**
Officers, volunteers and Museum staff with access to the data must receive data protection training to explain how they should store and handle personal information and a record kept of such training on a signed form as shown at Appendix A. Refresher training should be provided at regular intervals for existing users and logged on a form as Appendix B.

3 **Use strong passwords**
There is no point protecting the personal information we hold with a password if that password is easy to guess. All passwords must contain upper and lower case letters, a number and a symbol and be at least 8 characters long. This will help to keep information secure from would-be thieves.

4 **Encrypt all portable devices**
Make sure all portable devices – such as memory sticks and laptops – used to store personal information are encrypted.

5 **Only keep people's information for as long as necessary**
We must established a retention period and set up a process for deleting personal information once it is no longer required. This includes information held in a back-up

5 Data Held

Data falls into two broad categories: membership data and Gift Aid data. Membership data held may include some or all of the following:

1 Membership number
2 Title, name and decorations
3 Full postal address
4 E-mail address
5 Telephone number
6 Black Watch Association Branch
7 Membership type
8 Payment type
9 Bank account details
10 On-line and Shop receipts
11 Gift Aid request
12 Date joined
13 Membership year starting
14 Cocktail Party attendance
15 No marketing requested

Gift Aid data will include the following:

1 Title and name
2 Full postal address
3 Membership number

4 Date of registration

5 Date of last donation

6 Data Retention

Membership data will be held for 12 months following the expiry of membership

Gift Aid data will be held for 6 years following the last donation of for such period as is required by law whichever is the longer.

7 Required Practice

The Friends requires all its office bearers, volunteers and Museum staff to comply with the Act, the GDPR and this policy (and as each may be amended from time to time) when handling any Personal Data. No Sensitive Personal Data may be collected or retained.

There must be an annual assessment on the category of data held and the requirement to hold same. Such assessment must be logged on form as at Appendix C.

There must be an annual assessment of data for records that should no longer be held. Such assessment must be logged on form as at Appendix D.

Any officer, volunteer or Museum staff member may only be given access to the data following an assessed need to so access the data and following training on the requirements of the DPA and GDPR.

The storage of data on the Museum's server must be in a folder only accessible to officers, appropriate volunteers of the Friends and appropriate Museum staff, and accessible by a password fulfilling the definition of a strong password as in Section 3.

Any electronic data removed from the server must be held on an encrypted device.

Any data removed in hard copy must be kept secure and disposed of securely at the earliest opportunity.

Any index hard copy records must be held in a secure location.

Any office bearer or volunteer who considers that this policy has not been followed in any instance must contact the Chairman of the Friends.

8 Data Security Breach

We have to notify the Information Commissioner of any breach where it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

The Chairman of the Friends must be informed immediately if any data goes missing. An immediate investigation will be launched by the Chairman. Depending on the circumstances, consideration will also be given to making a report to the Information Commissioner.

The data will be salted with a minimum of three sets of trace data linked to Management Committee members. This data will contain markers that make it unique to the Friends dataset. In the event of the data appearing from any source other than the Friends the Chairman will be notified immediately and a report made to the Information Commissioner within 72 hours of the breach being detected.

9 Data transfer

Any transfer of the data outside of the Friends organisation will only be made when required for the purposes of the correct operation of the Friends organisation. No data containing identifiable personal data will be transferred outside of the European Economic Area except to an organisation operating a protocol considered by the EU Commission to be equivalent to GDPR.

10 Automated Decision Making

No automated decision making will take place on the data held by the Friends other than to comply with the request of an individual Member not to receive specific types of communication.