Friends of Bridge of Allan

Data Protection and Security Policy (compliant with the GDPR)

Introduction

Purpose

The Friends of Bridge of Allan (herein after referred to as the group) is committed to being transparent about how it collects and uses the personal data of its members, and to meeting its data protection obligations. This policy sets out the group's commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to the personal data of members. **This membership related personal data will not be shared with any third party, except as required by law, and will only be used for membership purposes.**

The group has appointed Douglas Neilson, Chair as the person with responsibility for data protection compliance within the organisation. He can be contacted at contact@friendsofbridgeofallan.co.uk. Questions about this policy, or requests for further information, should be directed to him.

Definitions

"Personal data" is any information that relates to an individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

Data protection principles

The group handles personal data in accordance with the following data protection principles:

- The group processes personal data lawfully, fairly and in a transparent manner.
- The group collects personal data only for specified, explicit and legitimate purposes namely membership records.
- The group processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- The group keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- The group keeps personal data only for the period necessary for processing.
- The group adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

- The group tells individuals the reasons for processing their personal data and how it uses such data. It will not process personal data of individuals for other reasons.

The group will update personal data promptly if an individual advises that his/her information has changed or is inaccurate.

Personal data gathered during the period of membership is held in hard copy and electronic format. The group will hold personal data until that person's membership ceases.

The group keeps a record of its processing activities in respect of personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

Individual rights

As a data subject, individuals have a number of rights in relation to their personal data.

Subject access requests

Individuals have the right to make a subject access request. If an individual makes a subject access request, the group will tell him/her:

- whether or not his/her data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom his/her data is or may be disclosed.
- for how long his/her personal data is stored (or how that period is decided);
- his/her rights to rectification or erasure of data, or to restrict or object to processing;
- his/her right to complain to the Information Commissioner if he/she thinks the organisation has failed to comply with his/her data protection rights; and
- whether or not the group carries out automated decision-making and the logic involved in any such decision-making.

The group will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless he/she agrees otherwise.

To make a subject access request, the individual should send the request to [email address]. In some cases, the group may need to ask for proof of identification before the request can be processed. The group will inform the individual if it needs to verify his/her identity and the documents it requires.

The group will normally respond to a request within a period of one month from the date it is received.

Other rights

Individuals have a number of other rights in relation to their personal data. They can require the group to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override the group's legitimate grounds for processing data (where the organisation relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the group's legitimate grounds for processing data.
- To ask the group to take any of these steps, the individual should send the request to [email address].

Data security

The group takes the security of personal data seriously. The group has a policy in place to:-

- protect personal data against loss, accidental destruction, misuse or disclosure and

Ensure that:-

- data is not accessed, except by members of the committee in the proper performance of their duties;
- personal data will not be transferred to any third party;
- any desk or cupboard containing personal data must be kept locked;
- computers storing personal data will be locked with a password or shut down when left unattended
- discretion is used when viewing personal data on a monitor to ensure that it is not visible to others;
- copies of personal data on paper or computer will be physically destroyed when no longer required.

Data breaches

If the group discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The group will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

Individual responsibilities

Individuals are responsible for helping the group keep their personal data up to date. Individuals should let the group know if data provided to the group changes, for example if an individual moves house or changes his/her email address.

Individuals may have access to the personal data of other individuals in the course of their volunteering. Where this is the case, the group relies on individuals to help meet its data protection obligations to members.

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and

Training

The group will provide training to all committee members about their data protection responsibilities.