# FRIENDS OF SALISBURY CATHEDRAL

## DATA PROTECTION POLICY

Key details:
- Policy prepared by the Chairman and Executive Secretary of the Friends
- Approved by the Friends Council 12th November 2015
- Policy became operational on 12th November 2015
- Review date: November 2018

**Introduction**

The Data Protection Act (DPA) sets out the framework for handling personal data. The EU General Data Protection Regulations (GDPR) came into force on 25th May 2018 and strengthens the DPA and both of these pieces of legislation requires that Personal Data is processed fairly and securely. The Information Commissioner's Office is the regulator and can issue substantial fines for serious data protection breaches.

Trustees are responsible for ensuring compliance with th these regulations. In addition to financial penalties, there is the potential for reputational damage. It is therefore important that Trustees can demonstrate their awareness of their legal duties and responsibilities in respect of data protection and that appropriate and proportionate measures are taken to protect the misuse of Personal Data.

The Association of the Friends of Salisbury Cathedral needs to gather and use certain information about its membership. The charity has a "Legitimate Interest" in collecting the personal data of both staff and members. This policy describes how this Personal Data must be collected, handled and stored to meet the charity's data protection standards — and to comply with the law.

**Why this policy exists**

This data protection policy ensures that the Friends of Salisbury Cathedral:
• complies with data protection law and follows good practice
• protects the rights of members, staff and partners
• is open about how it stores and processes individuals' data
• protects itself from the risks of a data breach

**Data protection law**

The Data Protection Act 1998, together with the General Data Protection Regulations, describes how the Friends must collect, handle and store personal information of its members. These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act and GDPR are underpinned by eight important principles. These say that personal data must:

1. be processed fairly and lawfully
2. be obtained only for specific, lawful purposes
3. be adequate, relevant and not excessive
4. be accurate and kept up to date
5. not be held for any longer than necessary
6. processed in accordance with the rights of data subjects
7. be protected in appropriate ways
8. not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

**Policy scope**

This policy applies to:

- the head office of the Friends
- all staff and volunteers of the Friends including the Cathedral departments and staff who share the personal data of the Friends membership
- all contractors, suppliers and other people working on behalf of the Friends
- all data that the Friends charity holds relating to identifiable individuals, even if that information technically falls outside of the General Data Protection Regulations

This can include:

- names of individuals
- postal addresses
- email addresses
- telephone numbers

…plus any other information relating to individuals

**Data protection risks**

This policy helps to protect the Friends from some very real data security risks, including:

- breaches of confidentiality. For instance, information being given out inappropriately.
- failing to offer choice. For instance, all individuals should be free to choose how the Friends uses data relating to them.
- reputational damage. For instance, the Friends could suffer if hackers successfully gained access to sensitive data.

**Responsibilities**

Everyone who works for or with the Friends has some responsibility for ensuring data is collected, stored and handled appropriately.

Each individual that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, the following people have key areas of responsibility:

1. **The Council of Trustees** is ultimately responsible for ensuring that the Friends meets its legal obligations.
2. **The Executive Secretary**, as the Data Protection Officer, is responsible for:

- keeping the board updated about data protection responsibilities, risks and issues.
- reviewing all data protection procedures and related policies, in line with an agreed schedule.

- arranging data protection training and advice for the people covered by this policy.
- handling data protection questions from staff and anyone else covered by this policy.
- dealing with requests from individuals to see the data the Friends holds about them (also called 'subject access requests').
- checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

3. **The IT provider** is responsible for:
- ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- performing regular checks and scans to ensure security hardware and software is functioning properly.
- evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.

**The Executive Secretary** is also responsible for:
- approving any data protection statements attached to communications such as fliers, forms, emails and letters.
- addressing any data protection queries from journalists or media outlets like newspapers.
- where necessary, working with other staff to ensure marketing or fundraising initiatives abide by data protection principles.

**General staff guidelines**
- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line manager.
- The Friends will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees of the Friends should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

**Data storage**
These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Executive Secretary -as Data Protection Officer.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.
These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:
- when not required, the paper or files should be kept in a locked drawer or filing cabinet.
- employees should make sure paper and printouts are not left where unauthorised people

could see them, like on a printer.
- data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:
- data should be protected by strong passwords that are changed regularly and never shared between employees.
- if data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.
- servers containing personal data should be sited in a secure location, away from general office space.
- data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
- data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- all servers and computers containing data should be protected by approved security software and a firewall.

**Data use**
Personal data is of no value to the Friends unless the charity can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- when working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
- data must be encrypted before being transferred electronically. The Executive Secretary can explain how to send data to authorised external contacts.
- personal data should never be transferred outside of the European Economic Area.
- employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

**Data accuracy**
The law requires the Friends of Salisbury Cathedral to take reasonable steps to ensure data is kept accurate and up to date.
The more important it is that the personal data is accurate, the greater the effort the Friends should put into ensuring its accuracy.
It is the responsibility of all who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.
- Data must be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a members details when they call.
- The Friends must make it easy for members to update the information the Friends holds about them. For example; by response sheet at membership renewal.
- Data should be updated as inaccuracies are discovered. For instance, if a member can no

longer be reached on their stored telephone number, it should be removed from the database.
- It is the Executive Secretary's responsibility to ensure the membership database is checked against industry suppression files every six months.

**Subject access requests (SAR)**
All individuals who are the subject of personal data held by the Friends are entitled to:

- ask what information the Friends holds about them and why.
- ask how to gain access to it.
- be informed how to keep it up to date.
- be informed how the Friends is meeting its data protection obligations.

If an individual contacts the Friends requesting this information, this is called a subject access request (SAR).

Subject access requests from individuals should be made by email, addressed to the Executive Secretary as Data Protection Officer who can supply a standard request form, although individuals do not have to use this. The Friends office will aim to provide the relevant data within 14 days. The Data Protection Officer will always verify the identity of anyone making a subject access request before handing over any information.

**Disclosing data for other reasons**
In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, the Friends will disclose requested data. However, the data protection officer will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

**Providing information**
The Friends aims to ensure that individuals are aware that their data is being processed, and that they understand:
- How the data is being used
- How to exercise their rights

To these ends, the charity has a privacy statement, setting out how data relating to individuals is used by the Friends, which is available on request.

Chairman 8th November 2018