Wakefield Gilbert and Sullivan Society
Data Protection Policy

Introduction

The 1998 Data Protection Act (DPA) applies to all the personal data held by Wakefield Gilbert and Sullivan Society (henceforth, "The Society"). It establishes a framework of rights and duties which are designed to safeguard personal data. By following this Data Protection Policy (DPP), we should meet our legal obligations. A summary of the DPA has been prepared as a separate document. You can also get more information from the Information Commissioner's Office or at www.ico.gov.uk.

Definitions of Personal Data from the Information Commissioner's Office:

"Personal data means data which relate to a living individual who can be identified –
(a) from those data, or
(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller [Wakefield Gilbert and Sullivan Society] and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual."

"Sensitive personal data means personal data consisting of information as to -
(a) the racial or ethnic origin of the data subject,
(b) his political opinions,
(c) his religious beliefs or other beliefs of a similar nature,
(d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
(e) his physical or mental health or condition,
(f) his sexual life,
(g) the commission or alleged commission by him of any offence, or
(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings."

Reasons for holding personal data

The Society needs to hold personal data about its associates. By 'associate' we mean **anyone who chooses to be associated with us, rather than being paid.** We need to be able to contact our members, patrons and vice-presidents and keep records about their subscriptions and insurance. We need to be able to contact other associates who are involved with The Society. We need to keep a list of subscribers to our newsletter through which we market our activities.

We do not need and will not hold any sensitive personal data. If it does become necessary to hold sensitive personal data, we will have to meet further obligations under the DPA, and our DPP will have to be revised.

Our Policy Principles

- Data will only be used to administer and market The Society.
- We will not use our data in any way which might adversely affect the individuals about whom we hold data.
- The Society will only hold the minimum amount of personal information necessary.

- Personal information will only be kept as long as it is needed.
- We will not collect sensitive personal information.
- We will not release personal data to any third party without the express permission of the associate. We will not share our lists of data.
- Data will be accessed on a “need to know” basis only, usually by committee members.
- We are committed to ensuring that, in principle, associates are aware that their data is being processed and: a) for what purpose it is being processed, b) what types of disclosure are likely; and c) how to exercise their rights in relation to the data.
- This policy will be reviewed every three years.

Who is responsible?

- The Chairman is responsible for ensuring information security.
- Members of the committee should be familiar with the legislation. This can be achieved by issuing the DPP and supporting documents to all committee members.
- The Secretary is responsible for ensuring information accuracy.

Collecting Data

- We will only collect data that has been agreed with the associate.
- We will always provide a Privacy Notice when we ask for data. This is attached as Appendix One. It will be provided with all electronic communications, or as a hard copy with the first contact made with a new associate.

Accuracy

Accuracy in our data is important to avoid irritating associates or causing harm to individuals. However, as the data we hold is not sensitive, inaccuracies do not pose significant risks.

We will aim to ensure that the data we hold is accurate and up-to-date by:

- Collecting only the minimum amount of data necessary.
- Asking individuals to provide their own personal data rather than obtaining it from other sources.
- Asking individuals to take responsibility for informing us of changes to their data.
- Holding data in as few central lists as possible, to avoid duplicate copies which risk not all being amended if data has to be updated.
- Encouraging committee members not to create additional unnecessary data sets.
- Editing data promptly when advised of inaccuracies.

Security

Only authorised people should be able to access, disclose or destroy personal data. Normally, data will only be accessed by committee members. Only the Secretary should disclose or destroy personal data.

Changes of committee personnel are a security risk. Care should be taken to ensure that:

- The DPP is issued to new committee members and that they understand their responsibilities.
- Data is securely transferred to the new officer responsible to ensure there is no loss of data.

- Personal data still held by the retiring member is securely destroyed (see Disposal of Data below).
- The change of personnel is reported promptly to associates and affiliated organisations so the retiring member does not continue to be sent personal data.

If personal data is accidentally lost, altered or destroyed, it should be possible for it to be recovered to prevent any damage or distress to the individuals concerned. This will be achieved in the following ways:

- Data held electronically should be backed up and stored in a different building to the computer, preferably in a fireproof location.
- Hard copies of personal data should be stored securely. The normal storage location should be a locked filing cabinet.
- Hard copies of personal data which are not in their usual storage place should be kept under supervision or on the officer's person to prevent theft, especially when in public places.

It is also a responsibility under the DPA that personal data is stored in a secure and confidential way.

- Personal Data will not be passed to any third party without the associate's permission.
- Committee members should be aware of the risk of being tricked into giving away information, especially over the phone. They should be careful not to give out contact information to a third party.

Electronic data is especially vulnerable to security risks and breaches of confidentiality.

- Electronic data should only be held on personal computers, not computers with public access.
- All computers used to store data should have up-to-date virus protection.
- All mailing lists should include the committee members, so they will be aware if there is any unauthorised use.
- As little personal data as possible will be made accessible online and only data that has already appeared in published programmes will be added to the public pages of the website.
- Website administrators are responsible for maintaining the confidentiality of their passwords, and if a breach is suspected, for changing their password.

The measures outlined above protect against accidental loss of data. They will also ensure that data is not lost through a security breach. However, in the case of a security breach, action should also be taken to ensure damage limitation.

- The extent of the breach should be investigated to determine what data is at risk.
- Immediate action applicable to the situation should be taken to prevent further damage.
- It may be necessary to notify associates that their data is at risk. This will alert them to be on their guard.
- Depending on the situation, it may also be necessary to inform the police or other agencies.
- Once the situation is stable, the circumstances of the breach should be assessed, and if necessary, better safeguards should be implemented. The DPP may need updating.

Subject Access to Data
All committee members should be able to recognise a "Subject Access Request" (SAR) and know how to deal with it. All individuals have a right to access the information held about them and request a copy. Such requests must be in writing, but need not employ any specific terms, so any request by an individual to know what is held about them is recognised as an SAR. SARs must be dealt with by The Society within 40 days. When SARs are received from individuals not personally known to The Society, their identity must be verified before releasing any data.

Individuals have the right to request that the data held about them is not used for direct marketing or that it is removed from the database. Such requests should be passed to the secretary and dealt with promptly.

Using Data

- Data will only be used for the purposes set out in this policy.
- We will not pass on any personal data from any data set to any third parties unless we have the express permission of the associate. This includes other members of the society. In the unusual situation that the society feels that it is necessary to break confidentiality (to comply with child protection legislation for example) this will be discussed by the committee and decided upon a case-by-case basis.
- Information about committee members will be made public according to their role, and consent will be sought for the method of contact they prefer to be made public.
- Information about associates will only be made public with their consent. Such data includes images. The membership form will ask for consent for associates' names and images to be published in performance programmes and on the website. Subscribers' names will not be made public.
- The list of subscribers to our newsletter will only be used for the circulation of newsletters. Newsletters may contain information (marketing) about events and products not provided by The Society as long as there is some link to our society.
- The committee will monitor the use of personal data held by the society, and if agreed to be necessary, update the DPP and ask the consent of associates to use their data in new ways.

Electronic mail is also regulated by the Privacy and Electronic Communications (EC Directive) Regulations 2003. We cannot send unsolicited marketing by electronic mail without getting the individual's permission first. Our Privacy Notice will ask permission to send marketing material in the form of our newsletters.

We will provide an opt-out option each time we email our subscribers. This will include the ability for the individual to reply directly to the message. Individuals can opt out of receiving marketing at any time and we will comply with any opt-out requests promptly. Our newsletters must also include the Society's contact details.

Disposal of data
When we no longer need to keep personal data, it will be destroyed securely. The entire committee will be informed that the data is no longer needed, so information can be removed from all datasets. Hard copies will be shredded. Electronic information will be deleted.

As we only hold a modest amount of personal data, we do not need a retention programme.

An archive of past performance programmes is maintained in both paper and electronic formats. This data will not be destroyed.

References

This DPP was prepared with reference to:

- Data Protection Policy Template provided by Lasa (London Advice Services Alliance), a charity providing ICT advice, consultancy and easy to read resources to the Voluntary and Community Sector obtained from http://ictknowledgebase.org.uk/dataprotectionpolicies
- "Data Protection Good Practice Note: Charities and Marketing" provided by Information Commissioner's Office available at www.ico.gov.uk
- "Data Protection Good Practice Note: Electronic mail marketing" provided by Information Commissioner's Office available at www.ico.gov.uk

Wakefield Gilbert and Sullivan Society
Data Protection Statement

The 1998 Data Protection Act (DPA) applies to all personal data held by The Society. It establishes a framework of rights and duties which are designed to safeguard personal data. The Society takes Data Protection seriously, and understands the requirement to meet the responsibilities of the DPA.

The Society needs to hold personal data about its associates to be able to contact them and to keep records about their subscriptions and insurance. By 'associate' we mean **anyone who chooses to be associated with us, rather than being paid.**

The Society has a Data Protection Policy and will abide by it.

Our Policy Principles

- Data will only be used to administer and market The Society.
- We will not use our data in any way which might adversely affect the individuals about whom we hold data.
- The Society will only hold the minimum amount of personal information necessary.
- Personal information will only be kept as long as it is needed.
- We will not collect sensitive personal information.
- We will not release personal data to any third party without the express permission of the associate. We will not share our lists of data.
- Data will be accessed on a "need to know" basis only, usually by committee members.
- We are committed to ensuring that, in principle, associates are aware that their data is being processed and: a) for what purpose it is being processed, b) what types of disclosure are likely; and c) how to exercise their rights in relation to the data.
- This policy will be reviewed every three years.

To see a complete copy of the DPP, please contact the Chairman:
Gordon Fawcett
Tel: 01924 339538
Email: chairman@wakefieldgilbertandsullivan.org.uk
Post: 63 Ferry Lane, Stanley, Wakefield, West Yorkshire, WF3 4JU

Data Protection Policy prepared by: Wakefield Gilbert and Sullivan Society Committee

Signed: .....(Chairman)

Date:.....

Appendix One
Wakefield Gilbert and Sullivan Society
Privacy Notice

Wakefield Gilbert and Sullivan Society needs to collect personal data about its associates to keep records about contact details, subscriptions and insurance. The data will be used by the committee to administer the society.

- **By becoming a member you agree that your name and images can be used in our performance programmes and on our website for perpetuity.**
- **By becoming a patron you agree that your name can be published in our performance programmes.**
- **By subscribing to our newsletter you agree that we can send you marketing material in the form of our newsletters.**

Other personal data will not be released to any third party without your permission. It is your responsibility to inform us of any changes to the data you provide. You can opt-out and request the data held about you to be deleted at any time by contacting the society. Please ask if you want to see a full copy of our Data Protection Policy. If you have any questions or suggestions, the Chairman can be contacted as follows:

Gordon Fawcett
Tel: 01924 339538
Email: chairman@wakefieldgilbertandsullivan.org.uk
Post: 63 Ferry Lane, Stanley, Wakefield, West Yorkshire, WF3 4JU