Honorary President: Glyn Bragg

DUNBARTONSHIRE CONCERT BAND

Dear Band Members

With the **General Data Protection Regulation (GDPR)** coming into force from 25th May 2018 we are required to gain your consent to keep and maintaining your personal data, and just opting out is no longer presumed to be consent of one kind or another.

Under the new legislation there have to be good reasons why we need to keep this information, and we have listed these below.

1) We want to be able to contact you with information about the band, concerts, dress code etc.

2) We want to be able to contact someone in the event of an emergency.

3) We need to keep a record of subscriptions and other payments for financial accounting purposes.

4) We want to be able to claim Gift Aid.

5) We want to be able to promote the band using names and photographs on our website, banners, programmes and social media or other formats that are appropriate. We also wish to retain an archive of band material, including names of past members and images, for historical purposes.

6) We want to be able to keep personal details of 'People to Contact' for arranging concerts at various venues or support us regularly so we can inform them of upcoming concerts.

7) Your data will only be kept by the current Chairman and Secretary of the Band and former Committee Members must pass **All** Data to the newly appointed Committee Members. Gift Aid details will be maintained by the current Treasurer. All personal details will be stored electronically and will be either password protected or encrypted.

8) Emails to band members will be concealed when group emails are sent out and will not be shared without your full written consent (not included on this form).

9) You are entitled to make a complaint if your feel there has been a breach of your personal data, by contacting the current Secretary/Chair.

Your rights:

1) You have the right to a copy of the information we keep on you.
2) You have the right to confidentiality of your personal information.
3) You have the right to see what information is stored about you.
4) You have the right to change any details.
5) You have the right to have your history deleted.
6) You have the right to complain about any data protection breach by contacting the current Secretary in writing stating what the breach is and for the appropriate action to be taken.

More Information

The text of the new EU General Data Protection Regulation (GDPR) has been finalised. When it comes into force it will replace all data protection legislation in EU member states (including the UK's Data Protection Act 1998 (DPA)) without the need for further national legislation.

The GDPR will apply to any entity offering goods or services (regardless of payment being taken) and any entity monitoring the behaviours of citizens residing within the EU. Companies are now directly responsible for data protection compliance wherever they are based (and not just their EU-based offices) as long as they are processing EU citizens' personal data.

Principles

The data protection principles, as set out in the DPA, remain but they have been condensed into six as opposed to eight principles. Article 5 of the GDPR states that personal data must be:

1. Processed fairly, lawfully and in a transparent manner in relation to the data subject.
2. Collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with those purposes.
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which data is processed.
4. Accurate and, where necessary, kept up to date.

5. Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.
6. Processed in a way 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.

Consent

Like the DPA, the GDPR will require data controllers to have a legitimate reason for processing personal data. If they rely on the consent of the data subject, they must be able to demonstrate that it was freely given, specific, informed and unambiguous for each purpose for which the data is being processed. Consent can be given by a written, including electronic, or oral statement. This could include the data subject ticking a box when visiting a website, choosing technical settings for social network accounts or by any other statement or conduct which clearly indicates their acceptance of the proposed processing of personal data. Silence, pre-ticked boxes or inactivity will no longer constitute consent.

Children

The preamble to the GDPR states: 'Children deserve specific protection of their personal data, as they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data. This concerns especially the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of child data when using services offered directly to a child.'

Article 8 requires that where the personal data of a child under 16 is being processed to provide 'information society services' (for example, online businesses, social networking sites and so on) consent must be obtained from the holder of parental responsibility for the child. Member states are allowed to lower this threshold where appropriate but not below the age of 13.

Data subjects' rights

The list of rights that a data subject can exercise has been widened by section 2 of the GDPR. The subject access right, rectification and being able to object to direct marketing remain. The right to have personal data processed for

restricted purposes and the right to transfer data/have it transferred to another data controller (data portability) are new rights.

In addition, article 17 introduces a 'right to be forgotten', which means data subjects will be able to request that their personal data is erased by the data controller and no longer processed. This will be where the data is no longer necessary in relation to the purposes for which it is processed, where data subjects have withdrawn their consent, where they object to the processing of their data or where the processing does not comply with the GDPR. However, the further retention of such data will be lawful in some cases where it is necessary for compliance with a legal obligation or for reasons of public interest in the area of public health or for the exercise or defence of legal claims.

To strengthen the 'right to be forgotten' online, the GDPR requires that a data controller who has made the personal data public should inform other data controllers which are processing the data to erase any links to, or copies or replications of, that data.

In brief – what does the Data Protection Act say about keeping personal data?

The Act does not set out any specific minimum or maximum periods for retaining personal data. Instead, it says that:

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

This is the fifth data protection principle. In practice, it means that you will need to:

- review the length of time you keep personal data;
- consider the purpose or purposes you hold the information for in deciding whether (and for how long) to retain it;
- securely delete information that is no longer needed for this purpose or these purposes; and
- update, archive or securely delete information if it goes out of date.

Website link: https://ico.org.uk