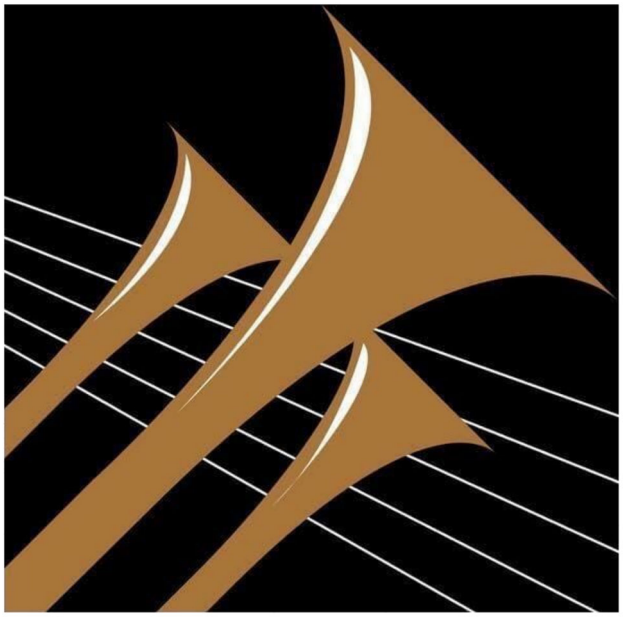

CITY OF BIRMINGHAM BRASS BAND

General Data Protection Regulation Guidelines

The General Data Protection Regulation (GDPR) came in to force on 25th May 2018. It is an EU law that sets out guidelines for the collection and processing of personal information and aims to give individuals more rights over how their data is used. These regulations apply to all types of organisations and although this legislation isn't 'aimed' at voluntary groups and charities, it does affect them and is something bands should be aware of.

Although GDPR is EU legislation and the UK is no longer a member of the EU, it is complemented by the UK's Data Protection Act 2018, which follows the same principles. The GDPR was also incorporated into the withdrawal agreement between the UK and the EU and continues to apply even after Brexit.

GDPR Guidelines

Personal data

The GDPR extended the rights individuals have over their data. For example, individuals now have the right to access, amend and object to the use of their personal data.

The definition of 'personal data' has been expanded to define anything that can be used to identify an individual; their name, postal address, bank details, ID/membership number, personal contact details or image (if you can identify someone on a photo/video this is now defined as their personal data).

Be aware of all the data you hold on someone.

Always think: *Could someone identify a person from this data?*

GDPR requires that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- processed in a manner 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.

(Guidance from the Information Commissioners Office, 2018)

Registered Charity No. 700361.
E: info@birminghambrass.co.uk W: www.birminghambrass.co.uk

GDPR Guidelines

Reason, consent and legitimate interests

When dealing with people's personal data, get into the habit of asking yourself about the following three things:

1. Reason

Under GDPR you should not be collecting data if there isn't good reason to do so. So unless you have legitimate reason for having and using data – don't ask for it.

- Consider the data you currently hold and decide if you need it.

2. Consent

Previously, consent could be implied by inaction or silence (a pre-ticked box or, 'unless you tell us otherwise we will email you'). Under GDPR consent will have to be proactive, i.e. an individual will have to take definitive action to say 'you can have and use my data' (e.g. they tick the box rather then it being pre-ticked). They should also have access to a clear and specific privacy statement that explains what the data they are providing will be used for.

- Change how you ask for consent.
- Historical opt-ins will need to be looked at.
- You may have to develop a few different privacy statements.

3. Legitimate interests

Some situations won't require positive consent as the use of data is implied. For example, emailing a member about a rehearsal change or a reminder about subs being due. This being said, members should still have access to clear and straightforward information about how their data will be kept and used.

- When someone provides data that will be used in this way, make sure privacy statements are readily available for them to read when they sign their data over.
- Regularly review (every year or every two years) the data you hold to decide if it is still relevant to your band.

GDPR Guidelines

Retention

Under GDPR you will have to be more careful about how long you keep data for; if you no longer need it, you shouldn't have it.

- Regularly review (every year or every two years) the data you hold to decide if it is still relevant to your band.

Secure storage of data

If you're storing information properly and securely then this shouldn't prove to be a problem. Rules around how you store data have not changed too much:

- Any electronically held data should be in a password-protected, secure environment, and passwords should be changed regularly, and with each personnel change (e.g. on the committee).
- It can be easy to focus on digital/electronic data but physically held data should be kept secure too. Keys should be kept track of/combination codes changed regularly and with each personnel change (e.g. on the committee).

Under GPDR you also need to consider how your data is stored by third parties, such as Google Docs or MailChimp. It is your responsibility to ensure they are compliant with GDPR.

Generally, larger organisations will have bases in the EU and will be GDPR compliant. Smaller organisations may be storing data outside of the EU so make sure you are aware of this.

- Review your storage policies as a matter of good practice.
- Think about which third parties you use (a quick internet search will tell you if they are aware of and on top of GDPR).

Documentation and processes

With GDPR, you must be able to show that you are compliant. So having policies, processes and privacy statements in place to show that you are treating data responsibly is important, as is having evidence of consent being given.

- Review and update your current documentation.

GDPR Guidelines

Does all this really apply to us?

Yes. From a band leader/committee member point of view GDPR might seem like a lot of unnecessary work for you but GDPR is there to protect individuals and to make sure organisations act responsibly. It applies to all organisations; from multi-national banks to local community organisations. Whilst a band is obviously different to a bank, people still have the right to expect that their data is well looked after.

Most of it is common sense and you don't need to get bogged down in the regulation. Just bear these two things in mind:

1. Getting a handle on things now will make things easier and help your group in the long run.
2. The spirit of GDPR: The overarching aim and spirit of GDPR is that individuals' data is treated fairly, reasonably and transparently. You may well be faced with a situation where there is a choice for you to make between the absolute letter of the law, and acting within the spirit of GDPR and the best interests of your group, and that's okay.

GDPR and children

The GDPR explicitly state that children's personal data merits specific protection. It also introduces new requirements for the online processing of a child's personal data.

Children have the same rights as adults over their personal data. These include the right to:

- be provided with a transparent and clear privacy notice which explains how their data will be processed;
- be given a copy of their personal data;
- have inaccurate personal data rectified and incomplete data completed;
- exercise the right to have personal data erased if they wish.

A child may exercise these rights on their own behalf as long as they are competent to do so. In Scotland, a person aged 12 or over is presumed to be of sufficient age and maturity to be able to exercise their data protection rights. In England and Wales and Northern Ireland, competence is assessed depending upon the level of understanding of the child.

Even if a child is too young to understand the implications of their rights, they are still their rights, rather than anyone else's such as a parent or guardian.

(Information Commissioners Office, 2018)

GDPR Guidelines

Children's data online

The provisions of GDPR help children to keep themselves safe online by giving them more control over the information they share.

GDPR gives children the 'Right to Erasure'. This means they can request online platforms to remove their personal data, including pictures, text or status updates.

If a child has shared any material online that they no longer wish anyone to see, they have a legal right to get this material removed, even if the content was posted by someone else.

GDPR and child protection

GDPR emphasises the importance of asking children for consent before sharing personal information.

If a child is mature enough you should give them the opportunity to decide whether they agree to their confidential information being shared. If a child doesn't have the capacity to make their own decisions, you should ask their parent or carer (unless this would put the child at risk).

If you have a child protection concern, you must share information with the relevant agencies, even if you haven't been given consent. GDPR does not affect this principle.