City of Bradford Brass Band Organisation

GDPR Statement

Contents

1. Aims

Our bands aims to ensure that all personal data collected about players and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.
It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.
It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

4. The data controller

Our band processes personal data relating to players, trustees, members and others, and therefore is a data controller.

3. Definitions

Term	Definition
Personal data	Personal data only includes information relating to natural persons who: ● Can be identified or who are identifiable, directly from the information in question; or ● Who can be indirectly identified from that information in combination with other information.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: ● Racial or ethnic origin. ● Political opinions. ● Religious or philosophical beliefs. ● Trade union membership. ● Genetics. ● Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes. ● Health – physical or mental. ● Sex life or sexual orientation.
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data Controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than a representative of the data controller, who processes personal data on behalf of the data controller.
Data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

5. Roles and responsibilities

This policy applies to band members, trustees and musical directors and to external organisations or individuals working on our behalf. Members who do not comply with this policy may face disciplinary action.

5.1 Management Committee

The management committee has overall responsibility for ensuring that our band complies with all relevant data protection obligations.

5.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.
They will provide an annual report of their activities directly to the management committee and, where relevant, report to the committee their advice and recommendations on band data protection issues.
The DPO is also the first point of contact for individuals whose data the band processes, and for the ICO.
Our DPO is the VCB secretary and is contactable via email at andyhansen@virginmedia.com

5.3 All members

Band members are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy.
- Informing the band of any changes to their personal data, such as a change of address.
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure.
    - If they have any concerns that this policy is not being followed.
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way.
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area.
    - If there has been a data breach.
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals.
    - If they need help with any contracts or sharing personal data with third parties.

6. Data protection principles

The GDPR is based on data protection principles that our band must comply with.
The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed.
- Accurate and, where necessary, kept up to date.
- Kept for no longer than is necessary for the purposes for which it is processed.
- Processed in a way that ensures it is appropriately secure.
- This policy sets out how the band aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 ‘lawful bases’ (legal reasons) to do so under data protection law:

- The data needs to be processed so that the band can **fulfil a contract** with the individual, or the individual has asked the band to take specific steps before entering into a contract
- The data needs to be processed so that the band can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone’s life
- The data needs to be processed so that the band, as a charity, can perform a task **in the public interest**
- The data needs to be processed for the **legitimate interests** of the band or a third party (provided the individual’s rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to young players and we intend to rely on consent as a basis for processing, we will get parental consent where the member is under 13.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Members must only process personal data where it is necessary in order to do their roles.
When members no longer need the personal data they hold, they must ensure it is deleted or anonymised.

8. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a member that puts the safety of other members at risk.
- We need to liaise with other agencies – we will seek consent as necessary before doing this.
- Our suppliers or contractors need data to enable us to provide services to our members – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law.
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share.
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud.
- The apprehension or prosecution of offenders.
- In connection with legal proceedings.
- Where the disclosure is required to satisfy our safeguarding obligations.
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our members.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the band holds about them. This includes:

- Confirmation that their personal data is being processed.
- Access to a copy of the data.
- The purposes of the data processing.

- The categories of personal data concerned.
- Who the data has been, or will be, shared with.
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period.
- The source of the data, if not the individual.
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.
- Subject access requests must be submitted in writing, either by letter, email or fax to the DPO. They should include:
    - Name of individual.
    - Correspondence address.
    - Contact number and email address.
    - Details of the information requested.

If a band member receives a subject access request they must immediately forward it to the DPO.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of members at our band may not be granted without the express permission of the child. This is not a rule and a child's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification.
- May contact the individual via phone to confirm the request was made.
- Will respond without delay and within 1 month of receipt of the request.
- Will provide the information free of charge.
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary.

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the band member or another individual.
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests.
- Is contained in adoption or parental order records.
- Is given to a court in proceedings concerning the child.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time.
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances).

- Prevent use of their personal data for direct marketing.
- Challenge processing which has been justified on the basis of public interest.
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area.
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them).
- Prevent processing that is likely to cause damage or distress.
- Be notified of a data breach in certain circumstances.
- Make a complaint to the ICO.
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

Individuals should submit any request to exercise these rights to the DPO. If the band receives such a request, they must immediately forward it to the DPO.

10. Photographs and videos

On becoming a member of the band individuals or parents / carers of any members under the age of 18 are asked to give signed permission for photographs and/or videos to be used by the band. If permission is not granted or if at any time permission is withdrawn then the band will not use any photographic or video recordings that contain images of that individual.

Requests to withdraw permission should be sent to the secretary. If permission is withdrawn then the band will make best endeavours to delete any images it currently holds of that individual. Uses may include:

- Within band on notice boards and in band magazines, concert programmes, newsletters, etc.
- Outside of band by external agencies such as the band photographer, newspapers, campaigns.
- Online on our band website or social media pages.

When using photographs and videos in this way we will not accompany them with any other personal information about a child, to ensure they cannot be identified.

11. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge.
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6).
- Completing privacy impact assessments where the band's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process).
- Integrating data protection into internal documents including this policy, any related policies and privacy notices.
- The DPO will keep the committee and members appraised of data protection law, this policy, any related policies and any other data protection matters'.
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our band and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices).
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

12. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.
In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use.
- Papers containing confidential personal data must not be left in the band hall unless within the designated locked cupboard, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, bandmasters will keep it secure and on their person.
- Band members who store personal information on their personal devices are expected to follow the same security procedures as for band-owned equipment.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

13. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.
For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files.

14. Personal data breaches

The band will make all reasonable endeavours to ensure that there are no personal data breaches.
In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a band context may include, but are not limited to:

- A non-anonymised dataset being published on the band website.
- Safeguarding information being made available to an unauthorised person.

15. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.
This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our band's practice. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the management.