Youth Brass 2000 Data Protection Policy

General Statement of the Band's Duties and Scope

The band is required to process relevant personal data regarding members, volunteers, parents, as part of its operation and shall take all reasonable steps to do so in accordance with this Policy.

Data Protection Controller

The band has appointed a committee member as the Data Protection Controller (DPC) who will endeavour to ensure that all personal data is processed in compliance with this Policy and the Principles of the Data Protection Act 1998, The Freedom of Information Act 2000 and the Protection of Freedoms Act 2012 are also relevant to parts of this policy.

The band recognises The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) adopted 27 April 2016 and the application date of 25 May 2018.

The Principles

The band shall so far as is reasonably practicable comply with the Data Protection Principles (the Principles) contained in the Data Protection Act to ensure all data is:-

- Fairly and lawfully processed
- Processed for a lawful purpose
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than necessary
- Processed in accordance with the data subject's rights
- Secure
- Not transferred to other countries without adequate protection

Definitions

- The band is “Youth Brass 2000”.
- Parental consent, includes the consent of a guardian.
- Data Subject, an individual who is the subject of the personal data.

Personal Data

Personal data covers facts about an individual where that data identifies an individual.

Processing of Personal Data

Consent will be required for the processing of personal data, concurrent with the band’s legitimate interests.

From age 16 a player has the right to revoke or change this Consent, in which case they must reach a new agreement with the Data Processor regarding how their data is processed

Sensitive Personal Data

The band may, from time to time, be required to process sensitive personal data. Sensitive personal data includes data relating to medical information, gender, criminal records and proceedings.

Rights of Access to Information

Data subjects have the right of access to information held by the band, subject to the provisions of the Data Protection Act 1998 and the Freedom of Information Act 2000. Any data subject wishing to access their personal data should put their request in writing to the Administration Manager. The band will endeavour to respond to any such written requests as soon as is reasonably practicable and in any event, within 40 days for access to records and 21 days to provide a reply to an access to an information request. The information will be imparted to the data subject as soon as is reasonably possible after it has come to the band's attention and in compliance with the relevant Acts.

Accuracy

The band will endeavour to ensure that all personal data held in relation to all data subjects is accurate. Data subjects must notify the data processor of any changes to information held about them. Data subjects have the right in some circumstances to request that inaccurate information about them is erased. This does not apply in all cases, for example, where records of mistakes or corrections are kept, or records which must be kept in the interests of all parties to which they apply.

Enforcement

If an individual believes that the band has not complied with this Policy or acted otherwise than in accordance with the Data Protection Act, that person should notify the DPC.

Data Security

The band will take appropriate technical and organisational steps to ensure the security of personal data. All committee members will be made aware of this policy and their duties under the Act.
The band is required to respect the personal data and privacy of others and must ensure that appropriate protection and security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to all personal data.
An appropriate level of data security must be deployed for the type of data and the data processing being performed. In most cases, personal data must be stored in appropriate systems and be encrypted when transported offsite. Other personal data may be for publication or limited publication within the band, therefore having a lower requirement for data security.

External Processors

The band must ensure that data processed by external processors, for example, service providers, Cloud services including storage, web sites etc. are compliant with this policy and the relevant legislation.

Secure Destruction

When data held in accordance with this policy is destroyed, it must be destroyed securely in accordance with best practice at the time of destruction.

Retention of Data

The band may retain data for differing periods of time for different purposes as required by statute or best practices. Other statutory obligations, legal processes and enquiries may also necessitate the retention of certain data.
The band may store some data such as photographs and achievements etc. indefinitely in its archive.