BCMCS
BOLTON CATHOLIC MUSICAL & CHORAL SOCIETY

Proud Patron of Bolton Hospice
caring from the heart

www.bcmcs.co.uk

Affiliated to the National Operatic & Dramatic Association

Chairman: Kathryn Wilkinson
6 Everleigh Close, Harwood
Bolton, Lancashire, BL2 3HE
01204 419213

Treasurer: Anthony Wilkinson
6 Everleigh Close, Harwood,
Bolton, Lancashire, BL2 3HE
01204 419213

Secretary: Neville Grady
707 Bradshaw Road, Bradshaw,
Bolton, Lancashire.
01204 856977

Information Management policy

March 2021

The General Data Protection Regulation (GDPR) and the Data Protection Bill

The General Data Protection Regulation (GDPR) is a Europe-wide law which is part of a wider package of reform intended to modernise data protection laws. Although the UK is no longer a member of the EU, the provisions of the GDPR have been enacted into law by the UK Parliament's Data Protection Bill.

GDPR applies to all personal data, regardless of whether it is held electronically (on a computer system, in emails, in text messages etc.) or on paper. There are particularly stringent rules surrounding "special category" data such as personal identifiers, personal characteristics, special educational needs, health, religious beliefs, ethnic background, home address and biometric data. In addition GDPR explicitly states that children's personal data must be given proper protection.

BCMCS aims to comply with the six data protection principles set out in the GDPR which require that personal data is:

1. Processed lawfully, fairly and transparently

2. Collected for a specified, explicit and legitimate purpose

3. Adequate, relevant and limited to what is necessary (ie: proportionate) for the purpose it is being processed

4. Accurate and kept up to date, with every reasonable step taken to erase or rectify inaccurate personal data without delay

5. Held in a form that means the data subject can be identified for only as long as is necessary for the purpose for which the personal data is processed

6. Processed in a manner that ensures appropriate security of the personal data

Processing Personal Data

BCMCS processes the personal data of adults and young people aged 13 or above with their consent, or to enable the legitimate interests of the Society. When processing special category data BCMCS will also satisfy one of the special category conditions. Details of the legal bases, special categories of data and the special category conditions can be found in Appendix 1.

Privacy Notice - Fair Processing of Data

Under principle 4 of the GDPR, BCMCS has a duty to check that children, parents and carers information is accurate and up to date. It fulfils this duty by sending out a data collection form to members or parents/carers of school age children and young people on application to join the Society. (Forms for school-age members are updated annually). This form will also include a privacy notice which outlines:

• What information is held by the Society

• Why the information is held

• How long the information is held for

• Who the information is shared with

• How members including children and their parents/carers can access the information which is held about them.

BCMCS also has a duty to check that Management committee members' and Honorary members' information is accurate and up to date. It fulfils this by asking them to complete a data collection form. The form also includes a privacy notice.

Consent

Consent is the main legal base available to BCMCS to process personal data. The Privacy Notices make clear that consent can be withdrawn at any time and the method to do so is clear and accessible.

If consent is withdrawn, the Society will immediately cease processing the personal data.

There are additional provisions within GDPR regarding securing consent from children. Only children aged 13 or over are able provide their own consent. For younger children, consent would need to be provided by whoever holds parental responsibility for the child. In such cases, BCMCS will make reasonable efforts to verify that consent is given or authorized by a parent or guardian.

A separate Privacy Notice is issued to children which is written in clear and age-appropriate language.

Information Security

Under principle 6 of the GDPR, the Society has a duty to ensure that data is handled securely. To fulfil its obligations BCMCS will adopt the following to maintain data security:

• Sensitive or personal data must not be left unattended at, or on route to and from, rehearsal or performance venues.

• Portable and mobile devices used to store and transmit personal information must be password-protected.

• Sensitive or personal data must be securely deleted when it is no longer required.

• Paperwork that identifies individuals must be stored securely when not in use

• BCMCS members processing personal information should be appropriately trained.

Information Asset Register and Record of Processing Activity

An information asset register will be compiled and kept up to date. This will summarise each information asset BCMCS maintains and include a record of activities related to higher risk processing such as processing personal data that could result in a risk to the rights and freedoms of individuals, and the processing of special category data, or criminal convictions/offences.

The information documented in the information asset register must reflect the current situation as regards the processing of personal data and therefore will be regularly reviewed to ensure that it remains accurate and up to date.

Data Protection Impact Assessments

In order to ensure that all data protection requirements are identified and any associated risks are addressed, BCMCS will complete a Data Protection Impact Assessment (DPIA) when introducing a new, or revising an existing, system or process which involves processing personal data.

Data Protection Officer

As a registered charity, BCMCS has a duty under GDPR to appoint a Data Protection Officer to assist with monitoring internal compliance, inform and advise on the Society's data protection obligations and provide advice regarding Data Protection Impact Assessments (DPIAs).

Incident Reporting

GDPR introduces a legal duty to report certain types of personal data breach to the Information Commissioner's Office (ICO); this must be done within 72 hours of the Society becoming aware of the breach, where feasible, even if all details of the breach are not yet known.

In addition, the Society is required to inform the data subjects of the breach without undue delay if it is considered that there is a high risk of the breach adversely affecting their rights and freedoms.

In order to meet these requirements, any suspected and/or actual breaches of information security will be reported to the Society's Data Protection Officer immediately, and in any event within 24 hours of the Society becoming aware of the breach. The details of the incident will be used to determine whether the breach requires a report to the ICO and/or the data subjects, and, following investigation, to create a correctional plan to ensure that a similar incident does not happen.

Record Retention

The Privacy Notices give information about the retention of data.

The Right to be Forgotten

Under GDPR individuals have the right to have personal data erased, this is also known as the 'right to be forgotten'. There is a particular emphasis on the right to erasure if the request relates to data collected from children. The right to be forgotten is not absolute and only applies in certain circumstances.

An individual can make a request for data to be erased either verbally or writing. The Society will respond to such requests within 1 calendar month to advise of its decision and will provide a clear justification if it refuses the request.

Disclosure of personal information

Personal information will be disclosed to 3rd parties under the following conditions:

- Information sharing with Local Authority personnel where performing licences are required.
- Information sharing with professionals working with children to ensure the wellbeing of children
- Investigation of a crime
- Subject Access Request, assuming that the child in question is sufficiently mature to make such a decision.

Appendix 1

Processing Personal Data: Legal Basis, Special Category Data and Special Category Conditions

Legal Basis: The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

d) Vital interests: the processing is necessary to protect someone's life.

e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Special Category Data: GDPR identifies that some information is particularly sensitive and therefore needs extra protection:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Health
- Sexual life or orientation
- Genetic data (e.g. blood samples DNA)

• Biometric data to identify an individual (e.g. finger-prints, iris recognition)

• Financial information

Special Category Conditions: Under GDPR if you are processing special category data you need to meet a special category condition in addition to the legal basis identified above. The special category conditions are:

• The data subject has given explicit consent

• Necessary to protect the vital interests where the data subject is physically or legally incapable of giving consent

• The data has been made publicly available by the data subject

• Necessary for the purposes of preventative or occupational medicine, for example the assessment of the working capacity of an employee

• Required for exercising rights in the field of employment and social security or social protection

• Processing is carried out by a foundation or not-for-profit body in the course of its legitimate activities

• Necessary to process legal claims

• Necessary for archiving statistical or historical research which is in the public interest

• Necessary for reasons of substantial public interest on the basis of UK law which shall be proportionate to the aim pursued

Data relating to criminal convictions or offences: Under GDPR information relating to criminal convictions (includes all DBS checks even if they show no convictions/offences) can only be processed process if you are doing so in an official capacity or have specific legal authorisation to do so.