NCBF DATA PROTECTION POLICY

(HEADER PAGE)

Version History and Control Sheet

Document Title	Data Protection Policy
Version	1.0
Date of original Creation	11/05/2021
Date of Last Issue	
Author/s	Duncan Stubbs

Document History			
Version Number	**Purpose/Change Details**	**Author**	**Date**
1.0	Original drafted document	Duncan Stubbs	11/05/2021

Document Sign Off	**Approved by all Trustees**		
	Signature	Name	Date
Chairman			
Administrator			

Contents

1. Overview

The **General Data Protection Regulation** (**GDPR**) is one of the most wide-ranging pieces of legislation passed by the EU in recent memory. It was introduced to standardise data protection law across the single market and give people in a growing digital economy greater control over how their personal information is used.

GDPR governs the way in which we can use, process, and store personal data (information about an identifiable, living person).

Data subjects will now have the right to demand subject access to their personal information, and the right to demand that an organisation destroys their personal information.

2. Introduction

NCBF needs to gather and use certain information about individuals and volunteers. These can include secretaries, players, suppliers, business contacts, volunteers and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet NCBF's data protection standards – and to comply with the law. The definition **"Personal data"** applies to all data that NCBF holds relating to individuals no matter the method of contact face to face/mail/telephone/Website.

3. Why this policy exists

This Data Protection Policy ensures NCBF:

- Complies with Data protection laws including the General Data Protection Regulation (GDPR) and follows good practice
- Protects the rights of individuals and participating players
- Is open about how it stores and processes individual's data
- Protects itself from the risks of a data breach and takes appropriate action
- Updates and Regularly Reviews processes involving personal data and documentation

As part of our record of processing activities we document, or link to documentation, on:

- information required for privacy notices
- records of consent
- the location of personal data
- Data Protection Impact Assessment reports
- records of personal data breaches.

4. Policy Statement

NCBF not only intends to comply with its obligations under the Data Protection Act 1998 and GDPR, but also assures both volunteers and all other persons about whom it retains personal data, that personal data will be processed in compliance with the legislation and any Codes of Practice issued by the Information Commissioner.

Data will be stored in a secure, confidential, and appropriate manner. Data Protection guidance and training is made available to assist Officers and volunteers in complying with this policy.

The data will only be stored whilst relevant and will not be disclosed to any person without the data subject's personal written authority or unless required by law. Under Articles 5 & 16 of the GDPR individuals have the right to have inaccurate personal data rectified. NCBF will ensure an individual may be able to have incomplete personal data corrected and updated.

5. Data Protection Law

The Data Protection Act 1998 describes how organisations – including NCBF – must collect store and handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by key principles. These are:

- Lawfulness, transparency and fairness
- Only using data for the specific lawful purpose that it was obtained, the most lenient of which is legitimate interests
- Only acquiring data that we strictly need
- Ensuring any data we possess is accurate
- Storage limitation
- Integrity and confidentiality
- Accountability

NCBF understands the rights of the individual granted by the legislation. They are as follows:

- Right to be informed of how your data is being processed
- Right to access this data
- Right to rectify incorrect data
- Right to erase data
- Right to restrict processing of personal data
- Right to data portability – this means that as a business you will need to put in place a system by which you can quickly and easily compile all the personal data you hold on an individual and make it securely accessible to them
- Right to object to your data being processed
- Rights relating to automated decision making, including processing

We have included information about both the purposes of the processing and the lawful basis for the processing in our privacy statement.

6. Policy Scope

This policy applies to:

- The Elected Officers and Trustees of NCBF
- All bands participating at NCBF Festivals
- All volunteers of NCBF
- All contractors, suppliers and other people working on behalf NCBF

The definition "**Personal data**" applies to all data that NCBF holds relating to individuals, even if that information technically falls outside the Data Protection Act 1998. This can include:

- Names of individuals
- Postal Addresses
- E Mail addresses
- Telephone numbers
- Any other information relating to individuals

7. Accountability and Governance

NCBF will

- implement appropriate technical and organisational measures that ensure compliance, which will include internal data protection measures including relevant training and internal checks of processing activities
- maintain relevant documentation on processing activities
- implement measures that meet the principles of data protection by design and data protection by default
- create and improve security features on an ongoing basis.

8. Data Protection Risks

This policy helps to protect NCBF from potential data security risks, including:

- **Breaches of confidentiality**. For instance, information being given out inappropriately.
- **Failing to offer choice**. For instance, all individuals should be free to choose how NCBF uses data relating to them.
- **Reputational damage**. For instance, NCBF could suffer if hackers successfully gained access to sensitive data.
- **Transfer of Data**.

9. Responsibilities

Everyone who works for or with NCBF has responsibility for ensuring data is collected, stored and handled appropriately.

Each Officer that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, there are key areas of responsibility:

The Officers and Trustees are ultimately responsible for:

- Reviewing all data protection procedures and related policies
- Arranging data protection training and advice for the people covered by this policy
- Handling data protection questions from anyone covered by this policy
- Dealing with requests from individuals to see the data NCBF holds about them (also called subject access requests)
- Checking and approving any contracts or agreements with third parties that may handle NCBF's sensitive data
- Ensuring data storage meets acceptable security standards
- Performing regular checks – including the annual deletion of Registered players performing
- Evaluating any third-party services the charity is considering using to store or process data, for instance cloud computing or remote access to data

The Administrator is responsible for:

- Approving any data protection statements attached to communications such as e mails and letters
- Addressing any data protection queries from media outlets or the press
- Where necessary, working with others to ensure marketing initiatives abide by data protection principles

10. General guidelines

(more detailed guidelines can be found at Appendix 2)

- The only people able to access data covered by this policy should be those who need it for their work
- NCBF will provide training to all Officers to help them understand their responsibilities when handling data
- Officers should keep all data secure, by taking sensible precautions and following the guidelines below
- In particular, "strong" passwords must be used and they should never be shared
- Personal data should not be disclosed to unauthorised people, either internally or externally
- Data should be regularly reviewed and updated if it is found to be out of date - if no longer required it should be deleted and disposed of
- Confidential and sensitive data must never be shared or linked on social media

11. Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the privacy@ncbf.info
When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed for some reason:

- When not required, the paper or files should be kept in **a locked drawer or filing cabinet**
- Officers should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer
- **Data printouts should be shredded** and disposed of securely when no longer required

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts.

- Data should be **protected by strong passwords** that are changed regularly and never shared between Officers
- If data is **stored on removable media** (like CD or DVD or pen drives) these should be kept locked away securely when not being used - Personal Data may not be stored or moved in this method
- Data should only be stored on **designated drives and servers** and should only be uploaded to approved storage mechanisms
- Data should be **backed up frequently** - those backups should be tested regularly, in line with standard back up procedures
- All computers containing data should be protected by approved security software

12. Data Use

Personal data is of no value to NCBF unless relevant to the smooth operation of its events. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, Officers should ensure the screens of their computers are always locked when left unattended
- Personal data should not be shared informally, in particular, it should never be sent by email as this form of communication is not fully secure
- Personal data **should never be transferred outside of the European Economic Area**
- Always access and update the central copy of any data

13. Data Accuracy

The law requires NCBF to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort NCBF should put into ensuring its accuracy.

It is the responsibility of all Officers who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary** - Volunteers should not create any additional data sets
- Officers should take every opportunity to ensure data is updated - For instance confirming band contact details when they call
- NCBF will make it easy for data subjects to update the information NCBF holds about them
- Data should be **updated as inaccuracies are discovered**.
- Requests to remove and update NCBF records must be made within 28 days of receipt

14. Subject access requests

All individuals who are the subject of personal data held by NCBF are entitled to:

- Ask **what information** NCBF holds about them and why
- Ask **how to gain access** to it
- Be informed how **to keep it up to date**
- Be informed how NCBF is **meeting its data protection obligations**

If an individual or customer contacts NCBF requesting this information it is called a subject access request.

Subject access requests from individuals should be made in writing addressed to the address at Appendix 3. The data controller can supply a standard request form although individuals do not have to use this.

The data controller will aim to provide the relevant information within 14 days.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

15. Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances NCBF will disclose the requested data; however, the data controller will ensure the request is legitimate, seeking assistance from the board and from NCBF's legal advisers where necessary.

16. Providing Information

NCBF aims to ensure individuals are aware their data is being processed, and that they understand

- How the data is being used
- How to exercise their rights

To these ends NCBF has a Privacy Statement setting out how data relating to individuals is used by NCBF. This is made available on request and is also available on the NCBF web site.

Appendix 1 - Definitions

The following terms are used throughout this policy and its application. These definitions comply with those used within the Data Protection Act. Each term is therefore defined as follows:

"Data" is information which:

- is processed by equipment operating automatically in response to instructions given for that purpose
- is recorded with the intention that it should be so processed
- is recorded as part of a relevant filing system

"Relevant filing system" means any set of information which is not processed by means of equipment but is structured in such a way that specific information relating to a particular individual is readily accessible.

"GDPR "General Data Protection Regulation

"Personal data" is data consisting of information which relates to a living individual who can be identified from that information (or from that and other information) including any expression of opinion about the individual and any indications of the intention of NCBF or any other person in respect of that individual.

"Data Subject" is an individual who is the subject of personal data.

"Processing" is obtaining, recording, holding or carrying out any operation on data; such as the organisation, adaptation, alteration, retrieval, disclosure, dissemination, rearranging or destruction of the information or the data.

"Customer or client" is an individual who uses the services of NCBF.

"Data controllers" determine why personal data will be used and what for.

"Data processors" are individuals or companies that process personal data on behalf of the data controller.

Appendix 2 - Guidelines

1. Personal data should only be recorded using either:

   Official NCBF paperwork e.g. application form, or computer systems

   Or

   Local administrative systems which must be approved by the person responsible for your team (local systems are defined as those containing no more than an individual's name, address and contact telephone number.)
   (First and Third Data Protection Principles – *see para 5 of Policy*)

2. An individual's personal data must not be disclosed to a third party without consulting and gaining consent from the individual.
   (Second Data Protection Principle)

3. All data must be kept factual, clear and precise. Informal notes expressing subjective and unsubstantiated remarks are not acceptable.
   (Third, Fourth and Fifth Data Protection Principles)

4. All personal data must be kept secure at all times
   (Seventh Data Protection Principle):-
   - Care must be taken to ensure that the security of personal data is not breached by, for example, files being left unattended.
   - This particularly applies to information carried by volunteers when away from office premises.
   - Remember to only transport necessary and relevant information.
   - Security includes documents in transit i.e. post, fax, photocopier and disc.
   - All individuals are responsible for maintaining the confidentiality of their computer passwords and reporting to the DPO any breach of security immediately.
   - All home-based Officers will store personal records in a lockable storage device. Individuals should discuss their requirements with their line manager.

5. Personal information to be destroyed should be shredded.
   (Third, Fourth, Fifth and Seventh Data Protection Principles)

6. All requests for access to personal files/records must be made in writing (recommended format Appendix 3).
   (Sixth Data Protection Principle)

7. An individual's application to have data corrected or erased must be submitted in writing to the Festival Director at NCBF, 6 Colehurst Croft, Solihull, B90 4XQ
   (Fourth and Sixth Data Protection Principles)

8. In exceptional circumstances where personal information is to be transferred outside the UK then consultation must take place with the NCBF Data Protection Controller.
   (Eighth Data Protection Principle)

9. Any Officer who wishes to obtain new personal data must first consult the Data Controller for approval.
   (Second and Third Data Protection Principles)

10. Personal data cannot be used for purposes such as conducting questionnaires/surveys or mailing fundraising/marketing literature, without the Individual having given their consent.
    (First and Second Data Protection Principle)

    The following Individual's Rights as described by GDPR are adopted :-

    - Right to be informed of how your data is being processed
    - Right to access this data
    - Right to rectify incorrect data
    - Right to erase data
    - Right to restrict processing of personal data
    - Right to data portability – this means that as a business you will need to put in place a system by which you can quickly and easily compile all the personal data you hold on an individual and make it securely accessible to them
    - Right to object to your data being processed
    - Rights relating to automated decision making, including processing

Appendix 3 Access request document

NCBF
SUBJECT ACCESS REQUEST FORM (SAR)
GDPR/DATA PROTECTION ACT 1998

Under the GDPR/Data Protection Act 1998, you are entitled to request access to personal information held about you by the National Concert Band Festival. Completing this form will assist us in locating your information quickly and efficiently.

Before completing this form please read the notes at the end of the document

1. Details of the Data Subject

Title (Mr. Mrs. Ms. Other)	
Surname	
First Name(s)	
Date of Birth	
Address (No./Street)	
Address (Town/City)	
Post Code	
Telephone Number	
Email	
Previous address(es)	

2. Are you the Data Subject? (Please tick the appropriate response)

YES If you are the Data Subject, please go to question 5.
NO Are you acting on behalf of the Data Subject with their authority? If so please provide evidence that you are legally authorised to obtain this information, for example, a signed letter of authority.

3. Details of the person requesting the information (if not the Data Subject)

Title (Mr. Mrs. Ms. Other)	
Surname	
First Name(s)	
Date of Birth	
Address (No./Street)	
Address (Town/City)	
Post Code	
Telephone Number	
Email	

4. Please state your relationship with the Data Subject that leads you to make this request for information on their behalf, for example, parent, legal guardian, solicitor.

5. Please help us to narrow down your request by informing use which parts of NCBF might hold information on you or the data subject. Please tick from the list below the services that you require us to conduct a search on :

Band Administrator	Festivals/Workshops
Adjudicator	Supplier
Other – Please specify below	

6. Documents needed before we can process this application:

a) Evidence of Data Subject's identify; original proof of identity and address is required to ensure that we only give information to the correct person, for example, a valid photo ID driving licence or passport and a recent utility bill, bank statement or Council Tax bill (no photocopies please) showing your name and address. These should be provided by registered post.

b) Evidence of the Data Subject's consent, for example, form of authority (if you are making the request on behalf of another);

c) NCBF does not charge for processing the subject access request. However, we may charge a 'reasonable' fee when a request is manifestly unfounded or excessive, particularly if it is repetitive. Cheques should be made payable to NCBF.

7. Please read the following declaration carefully, then sign, and date it.

I ..... certify that the information supplied to NCBF on this application form is true. I understand that it is necessary for NCBF to confirm my/Data Subject's identify and it may be necessary to obtain more detailed information in order to locate the correct information.

Signature : .....

Date : .....

Please send your completed form (along with evidence of identify, and address) to:

NCBF, 6 Colehurst Croft, Solihull, West Midlands, B90 4XQ

Marked for the attention of the **Administrator**.

Notes:

Data Subject: The person that the information is about.

Proof of Identification: The reason we ask for proof of identification is to maintain the security of the information we hold about you. This will help ensure that we do not release your personal information to anybody else. Any documents you send to use will be returned to you.

Previous addresses: If the information you are requesting may have been collected whilst you were living at an address other than your current one, it may be useful to supply us with that address in order that we can access the information more quickly.

Locating your records: NCBF is a voluntary organisation dealing with a diverse range of individuals and groups of people. Completing this section will ensure that your request is delivered to the correct area of NCBF and therefore dealt with more quickly and efficiently.

NCBF will not release information without proper authority and reserves the right to request further proof of authority or identity if necessary.