Crouch End Festival Chorus

Crouch End Festival Chorus

Cyber Security Data Protection and Privacy Policy

Introduction

This policy has been commissioned by the trustees to ensure that as a charitable company Crouch End Festival Chorus (CEFC) meets its legal obligations under the relevant data protection legislation and follows recognised good practice in the processing and protection of personal and organisational data.

Scope

This policy relates to all data kept by CEFC about an individual and applies to all CEFC records. *Data protection and privacy* (DPP) is essentially all about the protection of the personal data of individuals – for us whether they are members, employees/contractors, donors, Friends of CEFC, or clients/audience. *Cyber security* relates to the ability to protect all our electronic files, organisational data and archives against cyber hacking and theft.

Purpose.

The purpose of this policy is to ensure that CEFC is:

- complying with the law
- following good practice
- protecting members and other individuals as outlined above
- protecting the organisation.

What the legislation requires

Legislation in 1998, 2003 and 2007 means that Data Protection and Privacy (DPP) now covers the majority of manual records (files, letters, cardex systems etc) as well as electronic records and electronic channels of communication (email, telephone and fax). The introduction of the EU General Data Protection Regulation (GDPR) in 2018 means that we now have significantly more legal liability if we are responsible for a breach.

Appendix 1 gives details of the areas permitted for charities to collect information. Note that charities such as ours are exempt from registering with the DPP Commissioners providing we meet specific criteria, but charities are still legally obliged to confirm to the principles outlined in ***Appendix 2.***

Cyber security

Human errors, hacker attacks and system malfunctions can cause great financial damage and jeopardise our reputation. For this reason, in ***Appendix 3*** we have provided instructions and guidance to authorised users on maintaining cyber security. Users are expected to comply and, if needed, will be offered support to enable them to do so.

Crouch End Festival Chorus

CEFC Policy statement

1. We will only keep data on individuals that is justified for the purposes of establishing or maintaining membership or support for CEFC and/or providing or administering other activities in order to fulfil the established purpose of the charity.

2. Permission to do so must be given explicitly by the individual concerned, either through signing on to an email distribution list or offering CEFC specific information with the knowledge of how it will be used. Note that individuals must opt in.

3. The information we keep may relate to information about individuals who are either members of CEFC or who have regular contact with the organisation. The 2018 regulations require that in all cases a privacy statement must be given to explain the purpose for collecting the data. The statements are aligned with the purpose for collection. **See Appendix 4.**

4. We will restrict any disclosures, other than those made with the consent of the individual, to those third parties which are necessary to fulfil the above purposes, for example the Charities Aid Foundation (CAF).

5. In line with the records retention policy, we will not keep personal data once the need has become either obsolete or after the relationship between CEFC and the individual ends, unless it is necessary to do so to comply with legislation (e.g. company register).

6. We will be open with individuals about what information is kept about them.

7. Individuals will have the right to view the information kept about them in order to correct any factual inaccuracies.

8. If we wish to collect keep what is classified as sensitive data[1] about an identifiable individual we will seek explicit permission from them to do so. We will only collect such information where it is justifiable to do so, e.g. in order to provide appropriate support to the member during choir activities for health and safety reasons.

9. Appropriate technical and organisational measures shall be taken to secure data against unauthorised or unlawful access and processing.

10. If performing abroad, we will not transfer personal data to other countries (except names of singers if required) unless it is necessary for travel/visa purposes.

11. We will not sell personal data to direct marketing companies.

[1] *Sensitive data is anything we may record about racial, ethnic origin, beliefs, health, sexual orientation and criminal convictions that can be identified back to an individual*.

12. Subscribers to our Friends and newsletter schemes will be invited to re-subscribe as a one-off exercise to ensure we have their documented consent, in line with the Act.

13. A monitoring process will be implemented to deliver the above standards, linking with the IT strategy and Records Retention policy.

14. This policy will be regularly reviewed by the Trustees, will be posted on the CEFC public website, and will be included in the pack given to all new members.

4 Appendices follow.

Appendix 1

As a charity we are permitted to collect data about individuals to support the following areas:

1. Staff Administration
2. Fundraising
3. Realising the Objectives of a Charitable Organisation or Voluntary Body
4. Accounts & Records
5. Advertising, Marketing & Public Relations
6. Information and Databank Administration
7. Journalism and Media
8. Processing for Not for Profit Organisations
9. Research
10. Volunteers

Appendix 2

Data Protection and Privacy Principles

1. Personal data shall be processed fairly and lawfully – i.e. the data subjects must be told who is collecting the information, and the purposes for which the data is being collected.

2. Personal data shall be obtained for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that/those purpose(s).

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose.

6. Personal data shall be processed in accordance with the rights of data subjects under the Act. Briefly, these rights are:

a) The right to have a copy of information held about them
b) The right to take action for compensation
c) The right to have inaccurate personal data corrected or erased.

Appendix 3

Guidance to authorised users on cyber security

1. Protect personal and company devices.
When you use your digital devices to access CEFC emails or accounts, you introduce a potential security risk to our data. We advise you to keep your computer, tablet and mobile phone secure. You can do this if you:

- Keep all devices password protected
- Choose and upload a complete antivirus software
- Ensure you do not leave your devices exposed or unattended
- Install security updates of browsers and systems as soon as updates are available
- Log into CEFC accounts and systems through secure and private networks only.

We also advise our users to avoid accessing internal CEFC systems and accounts from other people's devices or lending your own devices to others unless you have already protected any CEFC information.

If you are entitled to access our administrative systems you will be given the appropriate administration rights and any related passwords. You should follow the above instructions to protect your devices.

2. Keep emails safe
Emails often host scams and malicious software (e.g. worms.) To avoid virus infection or data theft, we recommend that you:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. "watch this video, it's amazing.")
- Be suspicious of click-bait titles (e.g. offering prizes, advice.) Check email and names of people you have received a message from to ensure they are legitimate.
- Look for inconsistencies or give-aways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)
- If you aren't sure that an email you receive is safe, do not open it.

3. Passwords
Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they won't be easily hacked, but they should also remain secret. For this reason, we recommend that you:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays).
- If you need to write your password down somewhere (for backup or succession management), keep the paper or digital document confidential in a separate folder and destroy it when work is done or you have handed over to your successor.
- Exchange these credentials only when absolutely necessary and preferably in person.
- When exchanging them in person isn't possible, you should prefer the phone instead of email, and only if you personally recognise the person you are talking to. Change passwords on an agreed regular basis.
- Turn off screens and lock devices when absent from your devices.

4. Transfer data securely
Transferring data introduces security risk. You must:

- Avoid transferring sensitive data (e.g. personal information, financial records) to other devices or accounts unless absolutely necessary.
- When mass transfer of such data is needed, it must be encrypted with a password as recommended above.
- Ensure that the recipients of the data are properly authorised people or organisations and have adequate security policies.

Appendix 4

4a. Data Privacy Statement for members

Crouch End Festival Chorus collects data about its members in order to run the choir. In line with GDPR 2018 regulations, we only collect information around our legitimate interests.

1. General administration to carry out the choir's purpose.
We hold your name, address, telephone numbers and email address. This is available to members of the committee and their teams (e.g. section helpers) who need to contact you and can only be used for the purpose of running the choir and communicating with you about choir matters. For back up purposes your encrypted data is held by more than one person.

2. Financial information.
The subscriptions manager holds information about your standing order or direct debits. This is confidential to the subscription manager and the finance lead and is not shared elsewhere.

3. Singer review
The Music Director and membership manager also hold the full details about the voice test/singer review which is shared with the singer review subgroup only at the three year reviews.

4. Group placements
The choir group that the Music Director places you in is shared with the engagements manager in order for them to issue invitations to engagements.

5. Demographic information
We do not currently hold any other demographic information about our members but the above information is essential as part of membership.

6. Duration
We hold your name and contact, singer review and payment details for the duration of your membership. If you are happy to remain in contact with us we retain your contact details only. For our archives we retain the names of retired singers, which includes the date they left CEFC and all names of singers who were on the company register for the statutory amount of time.

7. Sharing with third parties
The information we hold about you is not released to third parties unless you are participating in a gig (names only, and any special health and safety requirements required by the organisers to meet an individual member's needs).

8. Removing information
If you do not want us to retain any of this information after you leave, contact the General Manager to request that your information is deleted.

9. Correcting data.
You have a right to see any information held about you and to correct any factual inaccuracies. To do so contact the general manager: general.manager@cefc.org.uk

4b. Data Privacy Statement for Friends of CEFC

Crouch End Festival Chorus collects basic data about its Friends in order to run the Friends scheme. In line with GDPR 2018 regulations, we only collect information around our legitimate interests.

1. General administration to carry out the choir's purpose.
We hold your name, address, telephone numbers and email address. This is available to the Fundraising Manager (overall lead for the Friends scheme) and the

Friends scheme administrator, and your name is given to our concert programme editor for recognising your contribution in our programmes.

2. Financial information.
The finance team holds information about your standing order or direct debits. This is confidential to them and is not shared elsewhere.

3. Sharing with third parties
The information we hold about you is not released to third parties.

8. Removing information
If you resign from the scheme we will delete any information we hold after you leave.

9. Correcting data.
You have a right to see any information held about you and to correct any factual inaccuracies. To do so contact the general manager: general.manager@cefc.org.uk

4c. Data Privacy Statement for CEFC Newsletter subscribers

Crouch End Festival Chorus keeps the email addresses of subscribers to the newsletter in order to distribute it. We hold your preferred email contact only. The information we hold about you is not released to third parties. You can unsubscribe to this newsletter by emailing unsubscribe@cefc.org.uk .

Policy title	**Cyber security data protection and privacy policy**
Date adopted	October 2015
Frequency of review	Every three years
Last reviewed	February 2018
Last approved by Trustees	July 2018
Next review due	May 2021