CLIFTON VILLAGE HALL COMMITTEE (CVHC)

- PRIVACY POLICY -

Contents

1. Objectives & Aims
2. Your personal data – what is it?
3. Data Controllers that CVHC Work With?
4. Data Processor that CVHC Work With?
5. What personal data may be collected or processed?
6. How we may use 'sensitive personal data'
7. Do we need your consent to process your sensitive personal data?
8. CVHC will comply with data protection law
9. We use your personal data for some or all of the following purposes:
10. What are the legal bases for processing your personal data?
11. Sharing your personal data
12. How long do we keep your personal data?
13. Your rights and your personal data
14. Transfer of Data Abroad
15. Further processing not covered by this policy
16. Information & Cyber Security
17. Data Protection Impact Assessments (DPIA)
18. Subject Access Requests (SAR)
19. Data/Security Breaches
20. Contact detail & complaints
21. Changes to this Privacy Policy

1. Objectives & Aims

- This Privacy Policy encompasses a wider set of obligations for CVHC to be compliant with the General Data Protection Requirements ("GDPR"). It aims to provide you with understanding about the following areas of the GDPR

2. Your Personal Data – What is it?

- "Personal data" is any information about a living individual which allows them to be identified from that data (for example a name, photographs, videos, email address, telephone number, or address). Identification can be directly using the data itself or by combining it with other information which helps to identify a living individual.
- The processing of personal data is governed by legislation relating to personal data which applies in the United Kingdom including the General Data Protection Regulation (the "GDPR) and other legislation relating to personal data and rights such as the Human Rights Act.

3. Data Controllers that CVHC Work With?

- Contractors
- Charity Commission

4. **Data Processors that CVHC Work With?**

   - Venues4Hire.org
     - Data Processors are responsible directly to you for the processing and security of your data that we share with them. They have separate Privacy Policies which you can read via the following links to their website. Venues4Hire.org: Privacy Policy and GDPR Statement

5. **What personal data may be collected or processed?**

   - Names, titles, aliases, signatures, photographs;
   - Contact details such as telephone numbers, postal addresses, and email addresses;
   - Where they are relevant to the services provided by CVHC, or where you provide them to us, we may process demographic information such as gender, age, place of birth, marital status, nationality, employment/skills, business/organisation, hirer/advertiser, academic/ professional qualifications, hobbies, family composition, and dependants;
   - When you make payment to CVHC for activities, financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers;
   - The data we process may include "sensitive personal data", such as racial or ethnic origin, religious beliefs, political beliefs, or data concerning your personal life and/or: Details of accidents where injury/outcome has been recorded such as mental and physical health, medication or treatment received, third parties involved, etc.

6. **How we may use 'sensitive personal data'**

   - We may process sensitive personal data including, as appropriate:
     - in order to comply with legal requirements and obligations to third parties.
     - In limited circumstances, with your explicit written consent.
     - Where we need to carry out our legal obligations.
     - Where it is needed in the public interest.
     - Where it is a matter of life or death.
   - Less commonly, we may process this type of personal data where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

7. **Do we need your consent to process your sensitive personal data?**

   - This information will never be shared with other parties, except for the conditions shown above, whereby we would process the data under the legal basis of Vital Interests.
   - In very limited circumstances, we may approach you (or your representative) for your written Consent to allow us to process certain sensitive personal data.
   - If we do so, we will provide you with full details of the personal data that we need and the reason why we need it, so that you can carefully consider whether you wish to consent.

8. **CVHC will comply with data protection law which says the personal data we hold about you must be:**

   - Used lawfully, fairly and in a transparent way.

- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Processed relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept and then destroyed securely, including ensuring that appropriate technical and security measures are in place to protect your personal data from loss, misuse, unauthorised access and disclosure.

9. We use your personal data for some or all of the following purposes:

- Accounts & Audit records
- Administration of Advertisers contract
- Administration of Data Processor contract
- Administration of Hirers contract
- Build up a picture of how we are performing;
- Claims handling
- Collect feedback about our services and performance
- Complaints handling
- Contractual requirement
- Confirm your identity and suitability to provide services
- Financial/accounting/banking transactions
- Fund raising to support the charity's objectives
- General correspondence with you via post, email, telephone, social media
- Health & Safety (in particular relating to entries made in to the Accident Book)
- Insurance/contractual claims
- Keep you informed of news about Clifton Village Hall
- Legal requirement
- Legitimate Interests (of CVHC and for the benefit of the Community)
- Maintenance of website content
- Meet all legal and statutory obligations and powers including any delegated functions;
- Organising volunteers
- Perform a booking/advertising contract
- Performance of a contract for goods/services provided
- Pre-contract checks
- Prevent and detect fraud and corruption in the use of the charity's funds and where necessary for use by law enforcement functions
- Process invoices
- Process receipts
- Processing grants or applications for funding
- Safeguarding and Prevent responsibilities
- Send you communications in the Legitimate Interests of CVHC
- Send you communications which you have requested
- Sharing data with other Data Controllers that we work with, for example contractors/ third parties who supply goods and services to meet the conditions of hire
- Sharing data with our Data Processor(s)
- Understand your needs in order to provide/improve our services
- Vital Interests, as may arise/relate to Health & Safety, for example the Accident Book process

10. What are the legal bases for processing your personal data?

- CVHC is a community-service based charitable organisation and has certain duties and obligations.
- Your personal data is processed for: Compliance with a Legal Obligation; Legitimate Interests of CVHC, Performance of a Contract (including pre-contractual steps), Vital Interests as may pertain to Health & Safety (accident/injury reporting), and Consent where other bases do not apply.
- This Privacy Policy sets out your rights and CVHC's obligations to you.
- Sometimes the use of your personal data may require your (opt-in) consent. We will ask for that consent if no other legal bases apply.

11. Sharing your personal data

- Information about the third parties with whom CVHC may share your personal data. These third parties have an obligation to put in place appropriate security measures and will be responsible to you directly for the manner in which they process and protect your personal data. It is likely that we will need to share your data with some or all of the following (but only where necessary):
    - Our agents, suppliers and contractors.
    - Data Controllers shown under the heading "Data Controllers That CVHC Work With?"
    - Data Processors shown under the heading "Data Processors that CVHC Work With?"

12. How long do we keep your personal data?

- CVHC has adopted a Document Management Policy. We will keep some records permanently if we are legally required to do so. We may keep some other records for an extended period of time. For example, it is currently best practice to keep financial records for a minimum period of 8 years to support HMRC audits or to provide income/tax information.
- We may have legal obligations to retain some data in connection with the contracts we enter in to, or to defend or pursue claims. In some cases, the law imposes a time limit for such claims (for example 3 years for personal injury claims or 6 years for contract claims). We will retain some personal data for this purpose as long as we believe it is necessary to be able to defend or pursue a claim.
- In general, we will endeavour to keep data only for as long as we need it and are legally entitled to do so. This means that we will delete/dispose of it, whether in paper or electronic/digital form, once it is no longer needed.

13. Your rights and your personal data

When exercising any of the rights listed below, in order to process your request, we may need to verify your identity for your own security. In such cases we will need you to respond with proof of your identity before you can exercise these rights.

You have the following rights with respect to your personal data:

1) The right to access personal data we hold on you

- At any point you can contact us to request the personal data we hold on you as well as why we have that personal data, who has access to the personal data and where we obtained the personal data from. Once we have received your request we will respond within one month.

- There are no fees or charges for the first request but additional requests for the same personal data or requests which are manifestly unfounded or excessive may be subject to an administrative fee.

2) ***The right to correct and update the personal data we hold on you***
   - If the data we hold on you is out of date, incomplete or incorrect, you can inform us and your data will be updated.
   - We will respond within one month of receipt of the request, or (if later) within one month ofrecwipt of: any information requested to confirm your identity; a fee (levied only in certain circumstances)
3) ***The right to have your personal data erased***
   - If you feel that we should no longer be using your personal data or that we are unlawfully using your personal data, you can request that we erase the personal data we hold.
   - When we receive your request, we will confirm whether the personal data has been deleted or the reason why it cannot be deleted (for example because we need it for to comply with a legal obligation).
   - We will respond within one month of receipt of the request, or (if later) within one month ofrecwipt of: any information requested to confirm your identity; a fee (levied only in certain circumstances)
4) ***The right to object to processing of your personal data or to restrict it to certain purposes only***
   - You have the right to request that we stop processing your personal data or ask us to restrict processing. Upon receiving the request, we will contact you and let you know if we are able to comply or if we have a legal obligation to continue to process your data.
   - We will respond within one month of receipt of the request, or (if later) within one month ofrecwipt of: any information requested to confirm your identity; a fee (levied only in certain circumstances)
5) ***The right to data portability***
   - You have the right to request that we transfer some/all of your data to another Data Controller. We will comply with your request, where it is feasible to do so, within one month of receiving your request.
   - We will respond within one month of receipt of the request, or (if later) within one month ofrecwipt of: any information requested to confirm your identity; a fee (levied only in certain circumstances)
6) ***The right to withdraw your consent to the processing at any time for any processing of data to which consent was obtained***
   - You can withdraw your consent easily by telephone, email, or post (see contact information for CVHC shown below).
7) ***The right to lodge a complaint with the Information Commissioner's Office***.
   - You can contact the Information Commissioners Office on 0303 123 1113 or via email at https://ico.org.uk/global/contact-us/email/ or by post to the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

14. Transfer of Data Abroad

- Any personal data transferred to countries or territories outside the European Economic Area ("EEA") will only be placed on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts approved by the European Union.
- Our website facilities are accessible from overseas so on occasion some personal data, for example an advert placed by a regular hirer/advertiser, may be accessed from overseas.

15. Further Processing Not Covered By This Policy

- If we wish to use your personal data for a new purpose, not covered by this Privacy Policy, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions.
- Where and whenever necessary, such that other legal bases do not apply, we will seek your prior consent to the new processing.

16. Information & Cyber Security

- Information & Cyber Security is a legal principal concerned with every aspect of processing personal data, and not just storage or transmission. The Data Protection Act says: "Appropriate technical and organisational measures" shall be taken against unauthorised or unlawful processing of personal data, and against accidental loss, or destruction of, or damage to, that personal data. Organisations should have appropriate security to prevent the personal data held being accidentally or deliberately compromised"
- In particular CVHC will ensure that it will:
    - Design and organise security measures to fit the nature of the personal data held, and the harm that may result from a security breach to that data;
    - Be clear about who has responsibility for ensuring information security;
    - Have in place the right physical and technical security, backed up by robust policies and staff that are well-trained; and
    - Be ready to respond swiftly and effectively to any breach of security.
    - Allow only authorised people to access, alter, disclose or destroy personal data;
    - Allow authorised people to only act within the scope of their authority
    - Ensure that If personal data is accidentally lost, altered or destroyed, that it can be recovered from a secure back-up
    - Have in place security that takes account of the nature of the data, the risks involved in the way it is processed, and the harm and distress that might result from its improper use
    - Take management & organisational, physical, and technological considerations in to account when considering levels of risk and designing solutions, for example:
    - Management & Organisational: Setting & changing authority for access to data, spreading awareness to promote a culture of accountability for the protection of personal data, co-ordination between key people in the processes carried out, access to premises or equipment, provision for IT equipment repairs and disposal, training and continuity arrangements when new role holders take up office, procedures for the use of email and website maintenance.

- Physical: Personal data is kept under lock and key and away from hazards, protection against theft/loss/damage of equipment, protection against the theft/loss/damage or incorrect destruction of paper records, and the disposal of paper records as confidential waste.
- Technological: IT/Computer/Network security appropriate to the size and complexity of processes and volume of data on systems. CVHC is entitled to balance the costs of this provision against the risks. Where Trustees work from home CVHC will put in place measures to ensure that this does not increase the risk of compromise to security of personal data.

- "Cyber Security" refers to the body of technologies, processes and people-practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.
  - CVHC will ensure, as a minimum, that its systems and equipment benefit from protection by means of controlled User Names & Passwords, a Firewall, Network Security for both Wi-fi and 4G, and proprietary Anti-Virus software.
  - Trustees' are aware of risks posed by suspicious emails, and the high risks of conducting business on devices if they are attached to a 'public' network.
  - CVHC employs, wherever possible, an automated backup of its electronic data to secure cloud storage, and whatever devices are used to process personal data are set up receive automatic updates of both system and virus protection software.
- "Third parties" that CVHC share personal data with include: Data Processors (website provider), other Data Controllers such as Accountants, the Charity Commission, Health & Safety regulators, and Insurers. All our partners are duty bound to comply with the requirements of GDPR.
- Additional protection is delivered by CVHC ensuring that:
  - Electronic email communication is via secure email.
  - Data entry necessary to maintain the contents of its website is via secure on-line data-entry forms, as provided under contract by the Data Processor.
  - Where business is conducted by Trustees' using their own equipment and/or email accounts, or where on paper or verbal, that they are duty bound under the Privacy Policy to "ensure that appropriate technical and security measures are in place to protect your personal data from loss, misuse, unauthorised access and disclosure".
  - There is in place a Data Processor Contracts Policy, which ensures that CVHC have contractual obligations on the Data Processor to take steps to keep your personal data secure in a way that is compliant with the GDPR.

17. Data Protection Impact Assessments (DPIA)

- CVHC recognise that Data Protection Impact Assessments are mandatory in certain circumstances, and the committee will give consideration to whether a DPIA should be undertaken for any project that has a potential to challenge the balance between a data subjects' rights and the objectives/intended outcome of the project.:
- CVHC has adopted a DPIA policy which it will apply, where necessary, to guide considerations.

18. Subject Access Requests (SAR)

- CVHC has adopted a Subject Access Requests policy and procedure, which is published on our website, www.cliftonvillagehall.org.uk and provides an easily accessible mechanism

through which such a request can be submitted, whilst also defining the method and procedure by which CVHC will respond.

- Requests can be made in either paper or electronic format and should be directed for the attention of the Chairman. (see contact details below).
- CVHC will respond to a SAR within one month of receiving the request
- CVHC are required to verify the identity of the person making the request and substantiate the nature of the request before they can respond further. Valid forms of ID are listed in the SAR Policy.
- SAR's are free to request, however CVHC may on occasion determine a request to be excessive/repetitive, and if so, may refuse the request or otherwise charge a reasonable fee.

19.Data/Security Breaches

- CVHC has adopted a Data Breach Policy, and has in place a "data breach response plan" which included the following elements:
    - Containment and recovery - The response to the incident will include a recovery plan and, where necessary, procedures for damage limitation.
    - Assessing the risks - CVHC will assess any risks associated with the breach, as these are likely to affect what may need to do once the breach has been contained. In particular, we will assess the potential adverse consequences for individuals; how serious or substantial these are; and how likely they are to happen again.
    - Notification of breaches - Informing people about an information security breach can be an important part of managing the incident, but it is not an end in itself. CVHC will be clear about who needs to be notified and why. We will, for example, consider notifying the individuals concerned; the ICO; other regulatory bodies; and other third parties such as the police, banks and the media.
    - Evaluation and response - It is important that causes of the breach be evaluated but also the effectiveness of CVHC's response to it. If necessary, we will review and update our policies and procedures accordingly to those findings.
- CVHC recognises that a data breach of any size is a crisis management situation, which could put individuals and organisations at risk. Data security is not in isolation merely an Information Technology (IT) issue, it is an organisational risk, and any response to a breach may involve people from a number of roles within CVHC and its associated operational network and partners.
- CVHC will follow guidance laid down by the Information Commissioner's Office (ICO) relating to its core responsibilities of: Containment and recovery, Assessing the risks, Notification of breaches, and Evaluation and response.
- The Chairman will assume responsibility for the Data Breach Response Plan, informing the data subject, our partners or the ICO where it is necessary to do so. If it were deemed necessary the Chairman will appoint a qualified external and independent specialist to act on behalf of CVHC. The Chairman will remain independent and act with the rights and interests of the data subject at the centre. (see contact details below).

20. Contact Details & Complaints

- Where information is collected from our website, and associated email system:
  the website address is: www.cliftonvillagehall.org.uk
  the email address is: cliftonvillagehall@gmail.com
- For questions relating to this Privacy Policy you should contact the Chairman, Clifton Village Hall Committee. Details are available on our website: www.cliftonvillagehall.org.uk and are available from any Trustee/Committee Member, or by emailing the Chairman at cliftonvillagehall@gmail.com
- Alternatively, you have the right to lodge a complaint with the Information Commissioners Office ("ICO") on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.
- Fundraising Preference Service: In 2015 a Cross-Party Review of Fundraising Regulation agreed that a service should exist for members of the public to control the nature and frequency of direct marketing approaches that they receive, including fundraising communications. You can choose to stop email, telephone, post and/or text messages from a selected charity by visiting the Fundraising Preference Service website: https://www.fundraisingpreference.org.uk/

21. Changes to this Privacy Policy

We keep this Policy under regular review and we will place any updates on our website that can be reached at www.cliftonvillagehall.org.uk.

**** This Policy was last reviewed in January 2022.**