Penicuik Community Arts Association (PCAA)
Data Protection Policy and Procedures

Introduction

The PCAA is committed to a policy of protecting the rights and privacy of individuals.

The PCAA needs to collect and use certain types of Data in order to carry out its work. This personal information must be collected and dealt with appropriately.

The goal of the data protection policy is to depict the legal data protection aspects in one summarising document. It can also be used as the basis for statutory data protection inspections. This is not only to ensure compliance with the European General Data Protection Regulation (GDPR) and Data protection Act (DPA) 2018 but also to provide proof of compliance.

The Data Protection Act 1998 (DPA) governs the use of information about people (personal data). Personal data can be held on computer or in a manual file, and includes email, minutes of meetings, and photographs. The PCA will remain the data controller for the information held. The PCA directors, staff and volunteers will be personally responsible for processing and using personal information in accordance with the Data Protection Act.

Management committee members,staff and volunteers running the PCA who have access to personal information, will be expected to read and comply with this policy.

PCAA and the Information Commissioners Office

https://ico.org.uk/for-organisations/data-protection-fee/self-assessment/y/

Following the questions on this website, the PCAA is not liable to pay Information Commissioners Office Fees.

However:

- As with all things data protection- related, it is crucial that charities keep good records of decisions made to demonstrate compliance so that if the ICO asks questions a few years later, they can show that they considered data protection and explain the reason they took a particular action.
- It is equally important to keep data (and its security) under review, updating policies and procedures at appropriate intervals and deleting personal data no longer needed. Remember that what is appropriate in terms of security will depend on the type of data, the likely harm a breach might cause, and the effect on individuals involved.
- Finally, organisations should ensure they have appropriate technical and organisational measures in place to keep any personal data held secure. This covers a wide range of measures from regular staff training, to controlling access to premises and documents, to secure methods of storing and sending data.

Contents

1. **Purpose and Scope**

This policy provides a framework for ensuring that the PCAA meets its obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 18). It applies to all the processing of personal data carried out by the PCAA, including its management committee and volunteers.

The PCAA complies with data protection legislation guided by the six data protection principles.

In summary, they require that personal data is:

- processed fairly, lawfully and in a transparent manner.
- used only for limited, specified stated purposes and not used or disclosed in any way incompatible with those purposes.
- adequate, relevant, and limited to what is necessary.
- accurate and, where necessary, up to date.
- not kept for longer than necessary; and
- kept safe and secure.
  In addition, the accountability principle requires us to be able to evidence our compliance with the above six principles and make sure that we do not put individuals at risk because of processing their personal data. Failure to do so, can result in breach of legislation, reputational damage, or financial implications due to fines. To meet our obligations, we put in place appropriate and effective measures to make sure we comply with data protection law.

2 Information covered by Data Protection Legislation

The UK GDPR definition of "personal data" includes any information relating to an identified or identifiable natural living person.

Pseudonymised personal data is covered by the legislation, however anonymised data is not regulated by the UK GDPR or DPA 18, providing the anonymisation has not been done in a reversible way.

The PCAA does NOT store personal data which is more sensitive and is afforded more protection, this is information related to:

- Race or ethnic origin;
  - Political opinions;
  - Religious or philosophical beliefs;
  - Trade union membership;
  - Genetic data;
  - Biometric ID data;
  - Health data;
  - Sexual life and/or sexual orientation; and • Criminal data (convections and offences)

3. Our Commitment

The PCAA is committed to transparent, lawful, and fair proportionate processing of personal data. This includes all personal data we process about members, volunteers or those who work or interact with us.

- **Privacy Notices** - we publish a privacy notice on our website (Appendix 1) and provide timely notices where this is required. We track and make available any changes in our privacy notice. We also publish a volunteer privacy notice and keep it up to date.
- **Training** - we require committee members and regular administration volunteers whose role requires them to collect personal data to undertake induction training on information governance and security which they re-take every year.
- **Breaches** - we consider personal data breach incidents and have a procedure that is communicated to the committee. We assess whether we need to report breaches to the ICO as the Regulator of DPA. We take appropriate action to make data subjects aware if needed.
- The PCAA Chair takes overall responsibility for Data Protection, supported by the Membership Secretary and Secretary.

4. Data collection

Informed consent

Informed consent is when

- A Data Subject clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data
- and then gives their consent.

The PCAA will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form.

When collecting data, the PCAA will ensure that the Data Subject:

- Clearly understands why the information is needed
- Understands what it will be used for and what the consequences are should the Data Subject decide not to give consent to processing
- As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed
- Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress
- Has received sufficient information on why their data is needed and how it will be used

5. Data Storage

Information and records relating to service users will be stored securely and will only be accessible to authorised directors, staff and volunteers.

Information will be stored for only as long as it is needed or required statute and will be disposed of appropriately. Membership spreadsheets are stored on computer for four years, then deleted. Gmail and website subscribers contacts' email addresses are deleted if the contact requests "unsubscribe". In addition, an annual review of members will identify email addresses which have been inactive for two years or more. The membership secretary may contact these people to ask if they still wish to receive PCAA news, and if there is no reply, the email address will be deleted.

It is the PCAA's responsibility to ensure all personal and organisation data is non-recoverable from any computer system previously used within the organisation, which has been passed on or sold to a third party.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 1998.

Where PCAA personal data is stored

(i) Our website subscriber list is covered by the software - Wordpress Newsletter Plugin

The General Data Protection Regulation (GDPR) adopted by the European Union entered into force in May 2018. This regulation poses a set of rules for how we communicate and interact with prospects and customers within the European Union and it focuses also on data storage and protection. The GDPR introduced some substantial changes to the previous norms that regulated those matters.

The Newsletter plugin is fully compliant with GDPR.

(ii) Our online sales software ("Woocommerce") stores names, email addresses, phone numbers and postal addresses of anyone buying tickets or other PCAA merchandise online. This is to enable the PCAA to deliver items purchased, to advise of any cancellations in events, or to issue a refund if stock is exhausted.

(ii) Our "Manual" database of members is stored as follows:

Excel spreadsheet of current members, and past members for the previous four years. Members names, email addresses, phone numbers and postal addresses are stored.

This is for Gift Aid applications and records, and for invitations to PCAA events and workshops for past members.

Three copies of each are stored. One copy resides on the personal computer belonging to the PCAA membership secretary (currently Di Davies). The second resides on the personal computer belonging to the PCAA Chair (currently Sue Owen). The third resides on the personal

computer of Carol Mann (Treasurer) for Gift Aid claim purposes. All personal computers are protected by a password.

Bank account details for exhibiting artists and performers are stored on our internet banking system, so that the PCAA can make direct payments of sales and performance fees.

(iii) Contact lists on the PCAA Gmail system.

Four members of the committee have access to the PCAA Gmail account and share log-in details: Chair, Secretary, Membership Secretary and Treasurer.

6. Preparing for a personal data breach

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is accidentally lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

We understand that a personal data breach isn't only about loss or theft of personal data.

Recital 85 of the UK GDPR explains that:

"A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. You need to assess this case by case, looking at all relevant factors.

We have prepared a response plan for addressing any personal data breaches that occur.

Date from the spreadsheets or the email contact lists is only shared with the data owner's permission, For example if another PCAA member wishes to make contact with the owner.

The major breach that could occur is using the full members's contact group in a "To" or "cc" field instead of in the "bcc" field.

If such a breach occurs, a member of the PCAA committee (chair, secretary or membership secretary) will contact all individuals affected so they are informed, and request all recipients to delete the offending email with the email addresses in the "to" or "cc" fields.

It is envisaged that no major harm would occur in the event of a breach. The worst case scenario would be receipt of unwanted emails from a PCAA member or friend.

The only PCAA committee members who are involved with accessing personal data for legitimate PCAA business are Sue Owen (Chair), Di Davies (Membership Secretary), Carol

Mann (Treasurer) and Jackie McDonald (Secretary). Each of these committee members has received a copy of this policy and is aware of the breach procedure.

Responding to a personal data breach - summary

We consider that the likely risk to individuals as a result of a breach is minimal

We believe that rights and freedoms of individuals affected by a PCAA data breach at not at high risk.

We know we must inform individuals affected by a data breach without undue delay, even though personal risks are negligible

Even though PCAA data breaches are low risk and the PCAA will not need to report breaches to the ICO, we need to be able to justify this decision, and will document it. The internal report will contain the information normally given to the ICO about a breach.

- a description of the nature of the personal data breach including, where possible:
    - the categories and approximate number of individuals concerned; and
    - the categories and approximate number of personal data records concerned;
- the name and contact details of the PCAA Chair.
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

Even though PCAA data breaches are low risk and the PCAA will not need to report breaches to the ICO, we will provide information to individuals, will provide advice to help them protect themselves from its effects. We will give the individuals the name and contact details of the PCAA Chair, or other contact point where more information can be obtained; a description of the likely consequences of the personal data breach; and a description of the measures taken or proposed to deal with the personal data breach and, where appropriate, a description of the measures taken to mitigate any possible adverse effects.

If possible, you should give specific and clear advice to individuals on the steps they can take to protect themselves, and what you are willing to do to help them. Depending on the circumstances, this may include such things as:

- forcing a password reset;
- advising individuals to use strong, unique passwords; and
- telling them to look out for phishing emails or fraudulent activity on their accounts.

We document all breaches, even though they don’t need to be reported.

7. Information rights and Communications

Information Rights - the PCAA will respond to data access requests and other information rights requests.

Communications - We have a clear communication plan which seeks to embed a culture of privacy and risk orientation.

The Data Protection Officer on the management committee is:

Name _____Susan Owen_____

Contact Details ___penicuikarts.org@gmail.com_____

The Data Protection Officer is responsible for ensuring that the policy is implemented and has overall responsibility for:

- Ensuring that everyone processing personal information understands that they are responsible for following good data protection practice
- Ensuring that everyone processing personal information is appropriately trained to do so
- Ensuring that everyone processing personal information is peer-supervised
- Dealing promptly and courteously with any enquiries about handling personal information
- Regularly reviewing and auditing the ways the PCAA holds, manages and uses personal information
- Regularly assessing and evaluating the PCAA's methods and performance in relation to handling personal information
- Ensuring that all committee members and volunteers are aware that a breach of the rules and procedures identified in this policy may lead to action being taken against them

8. Disclosure

The PCAA may need to share data with other agencies such as the local authority, funding bodies and other voluntary agencies.

The Data Subject will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows the PCAA to disclose data without the data subject's consent.

These are:

1. Carrying out a legal duty or as authorised by the Secretary of State
2. Protecting vital interests of a Data Subject or other person
3. The Data Subject has already made the information public
4. Conducting any legal proceedings, obtaining legal advice or defending any legal rights
5. Monitoring for equal opportunities purposes – i.e. race, disability or religion
6. Providing a confidential service where the Data Subject's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill Data Subjects to provide consent signatures.

The PCAA regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.

The PCAA intends to ensure that personal information is treated lawfully and correctly.

Destroying personal data.

Personal data should only be kept for as long as it is needed, and then deleted or destroyed.

9. Further information

If members of the public have specific questions about information security and data protection in relation to the PCAA please contact the Chair on penicuikarts.org@gmail.com

The Information Commissioner's website (www.ico.gov.uk) is another source of useful information.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 1998.

In case of any queries or questions in relation to this policy please contact the PCAA Data Protection Officer.

Signed: _____

Dated: _____

Review Date: _____

Related items

- PCAA Volunteer Privacy Policy

10. Version History

Document created	18th April 2022
Revision 1 due date	31st October 2022

Appendix 1

PCAA Website Privacy Policy

Privacy Policy

Who we are

We are the Penicuik Community Arts Association, a registered charity serving the people of penicuik. Our website address is: https://www.penicuikarts.org.

Comments

Comments on posts and pages of our site are currently disabled as a default. Where on occasion, we do switch them on for a specific page or post, we we collect the data from visitor's posts shown in the comments form, and also the visitor's IP address and browser user agent string to help spam detection.

We also collect this same data for messages sent via our forms.

An anonymized string created from your email address (also called a hash) may be provided to the Gravatar service to see if you are using it. The Gravatar service privacy policy is available here: https://automattic.com/privacy/. After approval of your comment, your profile picture is visible to the public in the context of your comment.

Media

If you upload images to the website, you should avoid uploading images with embedded location data (EXIF GPS) included. Visitors to the website can download and extract any location data from images on the website.

Cookies

If you leave a comment on our site or complete one of our forms you may opt-in to saving your name, email address and website in cookies. These are for your convenience so that you do not have to fill in your details again when you leave another comment. These cookies will last for one year.

If you visit our login page, we will set a temporary cookie to determine if your browser accepts cookies. This cookie contains no personal data and is discarded when you close your browser.

When you log in, we will also set up several cookies to save your login information and your screen display choices. Login cookies last for two days, and screen options cookies last for a year. If you select "Remember Me", your login will persist for two weeks. If you log out of your account, the login cookies will be removed.

If you edit or publish an article, an additional cookie will be saved in your browser. This cookie includes no personal data and simply indicates the post ID of the article you just edited. It expires after 1 day.

Embedded content from other websites

Articles on this site may include embedded content (e.g. videos, images, articles, etc.). Embedded content from other websites behaves in the exact same way as if the visitor has visited the other website.

These websites may collect data about you, use cookies, embed additional third-party tracking, and monitor your interaction with that embedded content, including tracking your interaction with the embedded content if you have an account and are logged in to that website.

How long we retain your data

If you leave a comment, the comment and its metadata are retained indefinitely. This is so we can recognize and approve any follow-up comments automatically instead of holding them in a moderation queue.

For users that register on our website (if any), we also store the personal information they provide in their user profile. All users can see, edit, or delete their personal information at any time (except they cannot change their username). Website administrators can also see and edit that information.

We also hold data on our mailing lists for our newsletters. If you subscribe to receive our news by email, your name and email address are retained indefinitely until “unsubscribe” is requested.

Only our website administrators, approved by our committee can see and edit this information.

What rights you have over your data

If you have an account on this site, or have left comments, you can request to receive an exported file of the personal data we hold about you, including any data you have provided to us. You can also request that we erase any personal data we hold about you. This does not include any data we are obliged to keep for administrative, legal, or security purposes.

Where we send your data

Visitor comments may be checked through an automated spam detection service.

Using our online shop

Our shop is designed using the WooCommerce software.
By default, WooCommerce retains:
What products a customer ordered and when
Name, e-mail address, and phone number provided by the customer
Billing (and optionally: shipping) address entered by the customer
A note about payment method used by the customer
This information, like the rest of our WordPress installation’s data, is stored in our website host’s database.

Your personal data will be used by WooCommerce to process your order, support your experience throughout the website and for other purposes described above.

You can request a copy of your personal data from us (we use the WordPress Personal Data Exporter) or you can request that your data is deleted. However this will mean you will need to re-enter essential details (name & contact details) if you order from us again.

Appendix 2

PCAA Website Software (Wordpress) Privacy Policy

Who we are

We are the Penicuik Community Arts Association

Our website address is: https://www.penicuikarts.org.

Comments

We do not provide the facility for visitors to make comments on our website

Cookies

We do not provide a login or comment facility on our website, so cookies for these activities are not generated

Embedded content from other websites

Although we rarely do this, articles on this site may include embedded content (e.g. videos, images, articles, etc.). Embedded content from other websites behaves in the exact same way as if the visitor has visited the other website.

These websites may collect data about you, use cookies, embed additional third-party tracking, and monitor your interaction with that embedded content, including tracking your interaction with the embedded content if you have an account and are logged in to that website.

How long we retain your data

If you subscribe to receive our news by email, your name and email address are retained indefinitely until “unsubscribe” is requested.

Website administrators can see, edit and delete that information.

What rights you have over your data

If you have an account on this site, or have left comments, you can request to receive an exported file of the personal data we hold about you, including any data you have provided to us. You can also request that we erase any personal data we hold about you. This does not include any data we are obliged to keep for administrative, legal, or security purposes.

Where we send your data

No features are used which involve sending or sharing your data