community albums

building better communities through music and media

Data Protection and GDPR Policy

Purpose: This document aims to set out the duties that we have as an organisation in processing and management the data and information of service users, staff, trustees, volunteers, staff, job applicants and others that we have a relationship with.

Scope: This policy is to be followed by, and affects the conduct of, all staff, volunteers and trustees.

Definition of terms:

Breach: A data breach can occur at any point when handling personal data and Community Albums has reporting duties in the event of a data breach or potential breach occurring. Breaches which pose a risk to the rights and freedoms of the data subjects require to be reported externally.
Consent: Consent gives individuals control and choice in how their data is used. Only with positive consent, can we hold a person's personal data for the purpose in which intended.
Data processor: A third party entity that processes personal data on behalf of COMMUNITY ALBUMS (e.g. payroll, database host, credit card payment processor).
DPO: Data Protection Officer
GDPR: General Data Protection Regulation – the new legislation that all organisations must abide by
ICO: Information Commissioner's Office – the UK's independent authority set up to uphold information rights in the public interest.
Personal Data: Data from which a living individual can be identified by reasonable means either by that data alone, or in conjunction with other data held by Community Albums or public records
PIA: Privacy Impact Assessment. This is a process that will assist Community Albums in identifying and reducing the risks that our operations have on personal privacy of data subjects.
Privacy Notices: A statement given highlight what personal information is gathered and how/ when it will be used, stored and deleted.
Special Category Data: Personal data that is sensitive in its nature, for example medical records.

Policy Statement
In performing its operations, Community Albums needs to gather and use certain information about individuals: service users, staff, trustees, volunteers, donors, job applicants and others. We may also hold personal data that is sensitive and relates to information on medical grounds (genetics, biometrics, health records), racial or ethnic origin, religious beliefs, sexual orientation and other topics.

It is our commitment to hold and process this data within our privacy notices, as set out in our procedures below.

We respect individual's rights, as set out in GDPR. These are:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure (right to be forgotten)
- Right to restrict processing
- Right to data portability
- Right to object (to processing for direct marketing; scientific/historical research & statistics; or the performance of a legal task or Community Albums' legitimate interests)

- Right not to be subject to automated decision-making including profiling.

As part of our legal compliance, we will collect, handle and store personal data in accordance with:
- The General Data Protection Regulation (EU) 2016/679
- The Privacy and Electronic Communications Regulations 2018 (UK)
- The Data Protection Act 2018 (UK)

Standard Operating Procedures

Procedures for Responsibility
All representatives of Community Albums will be responsible for protecting data as they create, maintain, preserve or disposed of records in their agreed capacity.

The role of Data Protection Officer (DPO) has been given to Jan Sheldon (Operations Manager), and any data protection issues can be raised by contacting her at jan@communityalbums.com

The DPO has overarching responsibility and oversight of compliance by Community Albums with data protection laws. They will be responsible for:
- Monitoring compliance with Data Protection laws and this Policy;
- Co-operating with and serving as a contact for discussions with the ICO;
- Reporting breaches or suspected breaches to the ICO and data subjects where appropriate.
- Ensuring the following timescales for holding data are adhered to:

Data Description	Retention Period	Start of Period	Relevant Provision/Reason
Supporter's personal data	As long as they are active (regular giving and/or other engagement) or no longer than 12 months if not active	On giving consent	To provide contact and enable appropriate communication
Beneficiary personal data	6 months	End of project	To allow for any required contact afterwards if necessary
Staff Personal Data – Personal files, including training records and notes	7 years	Start of employment on an ongoing basis	To cover the time for civil legal action claims
Staff Financial Records - Payroll, Income Tax and pension information	7 Years	End of financial year the payment was made	Charities Act 2011 Section 131. Charities and Trustee Investment (Scotland) Act 2005 Section 44

Staff, trustee and volunteer reference, DBS and safeguarding information	Indefinitely	From point of reference checks	For ongoing safeguarding of those who our representatives come into contact with now or in the future
Documents proving the right to work in the UK	2 years	On leaving employment	Immigration Act 2016
Trustee personal data	10 years	Rolling basis	Charities Act 2011
Contact Information – Patrons / Volunteer	1 year	On agreeing to become Patron/ Volunteer	To enable contact and provide information as necessary
Supporter's financial information	7 years	From date of last donation	To meet legal financial obligations

Procedures for a 'confidentiality culture'
As above, all representatives are to be careful in handling any information that they come across. Particular focus is given to the following practical considerations:

- Only CEO, Directors or Operations Manager should open mail, unless addressed to a specific person
- Particular sensitivity is needed in relation to income from individuals, whatever the amount given.
- When taking phone donations, we will aim not to repeat the donor's card numbers back to them – but instead ask them to do so
- Donation forms need to be kept securely and processed as quickly as possible
- Keeping printed information locked
- Only CEO, Directors or Operations Manager and the Chair of Trustees will have access to personal data

Procedures for protecting online data
Community Albums will take the following precautions to ensure that our website is protected from online fraud or attacks by:

- Always ensuring that our software and hardware is secure
- Using strong, protected passwords
- Making sure our server is backed up by antivirus software
- Never storing private information, especially of donors, on public servers
- Checking our online bank account regularly
- Looking out for unauthorised use of our name and logo

Procedures for processing personal data
Processing personal data includes the collection, storage, retention and disposal of data. We will process personal data on behalf of data subjects as long as:

- Processing occurs with the consent of the data subject
- Processing is necessary for the performance of a contract between Community Albums and the

data subject or for entering into a contract with the data subject
- Processing is necessary for Community Albums' compliance with a legal obligation
- Processing is necessary to protect the vital interests of the data subject or another person
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of Community Albums' official authority
- Processing is necessary for the purposes of legitimate interests.

Community Albums will provide privacy notices to all data subjects whose personal data it holds. Privacy notices are provided to data subjects from the outset of processing their personal data.

Procedures for processing special category personal data

In the event that Community Albums processes Special Category Personal Data, it must do so in accordance with one of the following grounds of processing:

- The data subject has given explicit consent to the processing of this data for a specified purpose;
- Processing is necessary for carrying out obligations or exercising rights related to employment or social security;
- Processing is necessary to protect the vital interest of the data subject or of another person where the data subject is incapable of giving consent;
- Processing is carried out as part of Community Albums' legitimate activities, relates only to individuals with whom it has regular contact, and the personal data is not disclosed beyond Community Albums without data subjects' explicit consent;
- Processing relates to data made public by the data subject;
- Processing is necessary for the establishment, exercise or defence of legal claims, or whenever court are acting in their judicial capacity;
- Processing is necessary for reasons of substantial public interest;
- Processing is necessary for reasons of preventative or occupational medicine, public interest in the area of public health, or public interest in the areas of historic or scientific research.

Community Albums will refer to Article 9 of GDPR and Schedule 1 (parts 1 &2) of the Data Protection Act 2018 when establishing conditions for processing Special Category data, however it is not currently expected that we will use Special Category Data.

Procedures for Data Sharing
Personal data may be shared within Community Albums in order to deliver daily activities and contractual agreements.

As far as possible refrain from sharing personal information. However, where this is necessary (for example, where Community Albums is fulfilling a contractual service where it is required to submit personal data as part of its reporting, or to refer a service user to another organisation) Community Albums will obtain prior consent from the data subject.
- Where Community Albums shares personal data with a third party organisation, it shall require the third party to provide evidence of compliance with data protection legislation.

Further, Community Albums will take steps to ensure the secure transfer of personal data:

- We will only transfer personal data to other organisations where it is necessary to do so, where the appropriate consent has been given, and where we are satisfied that the recipient has appropriate measures in place to comply with data protection law.
- When transferring data electronically, we will use password protected documents/storage devices to ensure that the data remains secure in transit. Passwords will be given separately (eg: in a separate email, or via telephone).
- Where practical, personal data will be handed over in person (eg: at a case conference).

Procedures of managing consent

A data protection consent form will always be used. It will aim to set out a clear statement of what their information will be used for and offer them clear choices, putting them in control of how information about them might be used. It will always require a positive opt-in, whereby ticking or signing leads to information use and leaving blank leads to non-information use. Different consent types will require different approvals – for example use to email to send updates and use of photograph for a fundraising campaign.

Consent forms will also clearly remind people of how they can opt-out of their consent.

Evidence of consent will be kept by the DPO and clearly state who gave consent, when, how and what was promised to them by Community Albums.

Consent will be reviewed annually and anyone whose information is still held, but does not need to be, will be removed from the appropriate records.

Procedures for Data Storage and Security

All Personal Data held by Community Albums will be stored securely, whether electronically or in paper format.

a. Paper Storage

If personal data is stored on paper it should be kept in a secure place where unauthorised personnel cannot access it. When the Personal Data is no longer required it must be disposed of securely, by shredding or confidential-waste bins, to ensure it can no longer be linked to an individual.

b. Electronic Storage

Personal data stored electronically must also be protected from unauthorised use and access. If personal data is stored on removable media (CD, DVD, USB memory stick) then that removable media must be stored securely at all times when not being used. Personal data should only be stored on designated drives or servers. When personal data is stored on mobile devices, these devices are to be password protected and stored securely when not in use.

Procedures for Data Protection Breaches

If you know or suspect a data security breach has occurred or may occur, you should email jan@communityalbums.com as soon as possible, with 'Data Security Breach' in the subject line. Notification of the data security breach will be documented and dealt with appropriately.

If it is not appropriate to contact DPO, you should contact the ICO as soon as possible – and ideally within 72 hours:

Phone: 0303 123 1113
Website: https://ico.org.uk/make-a-complaint/

Depending on the severity of any breach reported to them, Community Albums will also consider whether it is appropriate to contact ICO as well.

Failure of staff not to act may lead to action.

When the DPO becomes aware of a breach, they will:

- Take immediate steps to establish whether a breach has in fact occurred.
- Contain the data breach and, as far as possible, recover, rectify, move or delete data that has been lost, damaged or disclosed.
- Assess and record the breach in the risk register. It needs to include:
    - What type of data was involved?
    - How sensitive was the data?
    - How much data is involved?

    - Who is affected (by categories and number of subjects)?
    - The likely consequences of the breach
    - What happened? (in as much detail as possible)
    - What could third parties do with the information?
    - What are the wider consequences to consider for Community Albums (for example loss of reputation)?
- Notify appropriate parties of the breach as appropriate, which could include the police, the ICO and/ or the subjects of the data
- Take steps to prevent future breaches

Procedures for ensuring data subject's rights

Right to be informed

Community Albums will inform individuals of their rights at the point at which they share their data. In addition to their rights, Community Albums will inform individuals about how we will use their data, how long we will retain it for, and the legal basis/bases for processing their data. Community Albums will do this by providing an appropriate privacy notice.

Right of access

Individuals have a right to access their personal data and any requests to do so (whether verbally or in writing) will be treated as subject access requests.

Upon receiving a subject access request, the following procedure will be followed:

- Staff receiving a subject access request will alert the DPO at the earliest opportunity, who will respond to the request or provide appropriate support to the staff member responding to the request.
- The date, individual making the request and nature of the request will be recorded.
- The request will be acknowledged at the earliest opportunity.
- We will check which format the individual would prefer to receive their data in and comply with their preference where possible.
- Where there is any doubt, the identity of the individual making the subject access request will be verified (for example, we may request photographic ID before releasing the data). If the request is made via a third party, we will require verification that the third party is authorised to act on the individual's behalf before releasing the data. If we need to verify legitimacy of a request, we will contact the individual or party making the request at the earliest opportunity.
- The request will be responded to within 28 days of receiving it.
- If the request is complex, we may extend the response time by a further 2 months. We will write to the individual explaining the reasons for this within 28 days of receiving the subject access request.
- In addition to the data requested in the agreed format, we will provide a copy of the appropriate privacy notice and an explanatory note where it would be difficult for the individual to make sense of the data otherwise.
- No fee will be charged for subject access requests, unless a request is manifestly unfounded or excessive.
- Where a request is manifestly unfounded or excessive, Community Albums reserves the right to refuse or to charge a reasonable fee. We will write to the individual within 28 days of receiving the request explaining our reasons for refusing or charging, and advising them of their right to complain to the ICO or to seek judicial remedy.
- In the case of children, subject access rights reside with the child, not the adult with parental responsibility, although in the case of very young children a parent may reasonably exercise these rights on the child's behalf. Once a child is mature enough to understand (in broad terms) what it is to make a subject access request, then any information requested should be given to the child, not the adult with parental responsibility. There is no prescribed age for this and therefore Community Albums will deal with child subject access requests on a case-by-case basis, with reference to ICO guidance, and taking advice from a DPO if appropriate.
- Wherever possible, data pertaining to an individual making a subject access request will be isolated from data about other people. However, where this is impossible, Community Albums will refuse to comply with the request unless:

- the other individual has consented to the disclosure; or
- it is reasonable to comply with the request without that individual's consent.

Community Albums will deal with such issues on a case-by-case basis, with reference to and advice from ICO if appropriate.

Right to rectification

COMMUNITY ALBUMS will make every effort to ensure the accuracy of data held on individuals. Where inaccuracies come to our attention, we will correct these at the earliest opportunity.

Right to erasure

Where an individual requests that Community Albums erases some or all of their personal data, we will log and respond to this request without undue delay and normally within one month of receipt. Where this information is held in our database, we will remove any identifying information from the records through redaction or anonymization.

Right to restrict processing

Where an individual requests that Community Albums restricts processing, we will log and respond to this request without undue delay and normally within one month of receipt. We will work with our data processors to determine effective systems for restricting processing on a case-by-case basis. We will inform individuals concerned before lifting a restriction on processing.

Right to data portability

Where an individual wishes to copy or transfer the data that Community Albums holds about them to another entity, we will log and respond to this request without undue delay and within one month of receipt. Where the request is complex, this may be extended to two months and we will inform the individual and explain why the extension is necessary within one month of the request. We will aim to comply with the request when this right applies, but also where the right does not apply but it is appropriate to do so. Data to be transferred will normally be provided as an encrypted or password-protected csv file.

Right to object

Where an individual objects to Community Albums using their personal data to undertake direct marketing, we will stop immediately. If the objection to Community Albums processing personal data for other purposes, we will seek guidance from the ICO and comply with individual's request where appropriate. If there is legitimate interest in withholding information, for example for safeguarding purposes, then we shall do so.

Right not to be subject to automated decision-making

Community Albums does not currently use automated decision-making.

Privacy Impact Assessment (PIA)

We will carry out a PIA before undertaking a new project or processing activity which poses a "high risk" to an individual's privacy. High risk can include, but is not limited to, activities using information relating to health or race, or the implementation of a new IT system for storing and accessing Personal Data, etc.

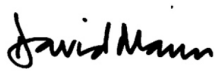
In carrying out a PIA, the following will be included in a brief report that is kept:

- A description of the processing activity
- Its purpose
- An assessment of the need for the processing
- A summary of the risks identified and the measures that could be taken to reduce those risks
- Details of any security measures that require to be taken to protect the personal data.

Community Albums will consult the ICO in the event that a PIA identifies a high level of risk which cannot be reduced. The DPO will be responsible for such reporting within five (5) working days.

This policy was agreed by the Board of Trustees on: 19th January 2023

Signed by: David Mann



Name/Role: Chair of trustees

This policy will be reviewed: 2026