Data Protection Policy

Overview

Key details

- Policy prepared by: Dundee Choral Union
- Approved by DCU Committee on: 29/01/2025
- Next review date: 30/01/2027

Introduction

In order to operate, Dundee Choral Union needs to gather, store and use certain forms of information about individuals.

These can include members, employees, contractors, suppliers, volunteers, audiences and potential audiences, business contacts and other people the group has a relationship with or regularly needs to contact.

This policy explains how this data should be collected, stored and used in order to meet Dundee Choral Union's data protection standards and comply with the General Data Protection Regulations (GDPR).

Why is this policy important?

This policy ensures that Dundee Choral Union:

- Protects the rights of our members, volunteers and supporters
- Complies with data protection law and follows good practice
- Protect the group from the risks of a data breach

Roles and responsibilities

Who and what does this policy apply to?

This applies to *all* those handling data on behalf of Dundee Choral Union e.g.:

- Committee members
- Employees and volunteers
- Members
- Contractors/3rd-party suppliers

It applies to all data that Dundee Choral Union holds relating to individuals, including:

- Names
- Email addresses
- Postal addresses
- Phone numbers
- Any other personal information held (e.g. financial)

Roles and responsibilities

Dundee Choral Union is the Data Controller and will determine what data is collected and how it is used. The Data Protection Officer for Dundee Choral Union is the General Secretary. They, together with the Committee are responsible for the secure, fair and transparent collection and use of data by Dundee Choral Union. Any questions relating to the collection or use of data should be directed to the Data Protection Officer.

Everyone who has access to data as part of Dundee Choral Union has a responsibility to ensure that they adhere to this policy.

Dundee Choral Union may use third party Data Processors (e.g. Mail Chimp) to process data on its behalf. Dundee Choral Union will ensure all Data Processors are compliant with GDPR.

Data protection principles

a) We fairly and lawfully process personal data in a transparent way

Dundee Choral Union will only collect data where lawful and where it is necessary for the legitimate purposes of the group.

- A member's name and contact details will be collected when they first join the group and will be used to contact the member regarding group membership administration and activities. Other data may also subsequently be collected in relation to their membership, including their payment history for 'subs'. Where possible, Dundee Choral Union will anonymise this data
    - Lawful basis for processing this data: Contract (the collection and use of data is fair and reasonable in relation to Dundee Choral Union completing tasks expected as part of the individual's membership).

- The name and contact details of volunteers, employees and contractors will be collected when they take up a position, and will be used to contact them regarding group administration related to their role.

  Further information, including personal financial information and criminal records information may also be collected in specific circumstances where lawful and necessary (in order to process payment to the person or in order to carry out a Protecting Vulnerable Groups (PVG) check).

    - Lawful basis for processing this data: Contract (the collection and use of data is fair and reasonable in relation to Dundee Choral Union completing tasks expected as part of working with the individuals),
- An individual's name and contact details will be collected when they make a booking for an event. This will be used to contact them about their booking and to allow them entry to the event.
    - Lawful basis for processing this data: Contract (the collection and use of data is fair and reasonable in relation to Dundee Choral Union completing tasks expected as part of the booking),

- An individual's name, contact details and other details may be collected at any time (including when booking tickets or at an event), with their consent, in order for Dundee Choral Union to communicate with them about and promote group activities. See 'How we get consent' below.
    - Lawful basis for processing this data: Consent (see 'How we get consent')

- Pseudonymous or anonymous data (including behavioural, technological and geographical/regional) on an individual may be collected via tracking 'cookies' when they access our website or interact with our emails, in order for us to monitor and improve our effectiveness on these channels. See 'Cookies on the Dundee Choral Union website' below.
    - Lawful basis for processing this data: Consent (see 'How we get consent')

b) We only collect and use personal data for specific, explicit and legitimate purposes and will only use the data for those specified purposes.

When collecting data, Dundee Choral Union will always provide a clear and specific privacy statement explaining to the subject why the data is required and what it will be used for.

c) We ensure any data collected is relevant and not excessive

Dundee Choral Union will not collect or store more data than the minimum information required for its intended purpose.

E.g. we need to collect telephone numbers from members in order to be able to contact them about group administration, but data on their marital status or sexuality will not be collected, since it is unnecessary and excessive for the purposes of group administration.

d) We ensure data is accurate and up-to-date

Dundee Choral Union will ask members, volunteers and staff to check and update their data periodically. Any individual will be able to update their data at any point by contacting the Data Protection Officer.

e) We ensure data is not kept longer than necessary

Dundee Choral Union will keep records for no longer than is necessary in order to meet the intended use for which it was gathered (unless there is a legal requirement to keep records).

The storage and intended use of data will be reviewed in line with Dundee Choral Union's data retention policy. When the intended use is no longer applicable (e.g. contact details for a member who has left the group), the data will be deleted within a reasonable period, as further defined in our Data Retention Schedule.

f) We keep personal data secure

Dundee Choral Union will ensure that data held by us is kept secure.

- Electronically-held data will be held within a password-protected and secure environment
- Passwords for electronic data files will be re-set each time an individual with data access leaves their role/position
- Passwords will be used for transfer of data between Committee Members
- Physically-held data (e.g. membership forms or email sign-up sheets) will be stored in a locked cupboard
- Keys for locks securing physical data files should be collected by the Data Protection Officer from any individual with access if they leave their role/position. The codes on combination locks should be changed each time an individual with data access leaves their role/position
- Access to data will only be given to relevant Committee members where it is clearly necessary for the running of the group. The Data Protection Officer will decide in what situations this is applicable and will keep a master list of who has access to data

g) Transfer to countries outside the EEA

Dundee Choral Union will not transfer data to countries outside the European Economic Area (EEA), unless the country has adequate protection for the individual's data privacy rights.

Individual rights

When Dundee Choral Union collects, holds and uses an individual's personal data that individual has the following the rights over that data. Dundee Choral Union will ensure its data processes comply with those rights and will make all reasonable efforts to fulfil requests from an individual in relation to those rights.

Individual's rights

- *Right to be informed:* whenever Dundee Choral Union collects data it will provide a clear and specific privacy statement explaining why it is being collected and how it will be used.

- *Right of access:* individuals can request to see the data Dundee Choral Union holds on them and confirmation of how it is being used. Requests should be made in writing to the Data Protection Officer and will be complied with free of charge and within one month. Where requests are complex or numerous this may be extended to two months

- *Right to rectification:* individuals can request that their data be updated where it is inaccurate or incomplete. Dundee Choral Union will request that members, staff and contractors check and update their data on an annual basis. Any requests for data to be updated will be processed within one month.

- *Right to object:* individuals can object to their data being used for a particular purpose. Dundee Choral Union will always provide a way for an individual to withdraw consent in all marketing communications. Where we receive a request to stop using data we will comply unless we have a lawful reason to use the data for legitimate interests or contractual obligation.

- *Right to erasure:* individuals can request for all data held on them to be deleted. Dundee Choral Union's data retention policy will ensure data is not held for longer than is reasonably necessary in relation to the purpose it was originally collected. If a request for deletion is made, we will comply with the request unless:
- There is a lawful reason to keep and use the data for legitimate interests or contractual obligation.
- There is a legal requirement to keep the data.

Right to restrict processing: individuals can request that their personal data be 'restricted' – that is, retained and stored but not processed further (e.g. if they have contested the accuracy of any of their data, Dundee Choral Union will restrict the data while it is verified).

Though unlikely to apply to the data processed by Dundee Choral Union, we will also ensure that rights related to portability and automated decision making (including profiling) are complied with where appropriate.

Member-to-member contact

We only share members' data with other members with the subject's explicit prior consent.

As a membership organisation Dundee Choral Union encourages communication between members.

To facilitate this:

- Members can request the personal contact data of other members in writing via the Data Protection Officer or General Secretary, where applicable. These details will be given, as long as they are for the purposes of contacting the subject (e.g. an email address, not financial or health data) and the subject has consented to their data being shared with other members in this way

How we get consent

Dundee Choral Union will regularly collect data from consenting supporters for marketing purposes. This includes contacting them to promote performances, updating them about group news, fundraising and other group activities.

Any time data is collected for this purpose, we will provide:

- A method for users to show their positive and active consent to receive these communications (e.g. a 'tick box')
- A clear and specific explanation of what the data will be used for (e.g. 'Tick this box if you would like Dundee Choral Union to send you email updates with details about our forthcoming events, fundraising activities and opportunities to get involved')

Data collected will only ever be used in the way described and consented to (e.g. we will not use email data in order to market 3rd-party products unless this has been explicitly consented to).

Every marketing communication will contain a method through which a recipient can withdraw their consent (e.g. an 'unsubscribe' link in an email). Opt-out requests such as this will be processed within 14 days.

Cookies on the Dundee Choral Union website

A cookie is a small text file that is downloaded onto 'terminal equipment' (e.g. a computer or smartphone) when the user accesses a website. It allows the website to recognise that user's device and store some information about the user's preferences or past actions. However, Dundee Choral Union does not store information from cookies on its website www.dundeechoralunion.org.uk

Data Retention Policy

Overview

Introduction

This policy sets out how Dundee Choral Union will approach data retention and establishes processes to ensure we do not hold data for longer than is necessary.

It forms part of Dundee Choral Union's Data Protection Policy.

Roles and responsibilities

Dundee Choral Union is the Data Controller and will determine what data is collected, retained and how it is used. The Data Protection Officer for Dundee Choral Union is the General Secretary. They, together with the Committee are responsible for the secure and fair retention and use of data by Dundee Choral Union. Any questions relating to data retention or use of data should be directed to the Data Protection Officer.

Regular data review

A regular review of all data will take place to establish if Dundee Choral Union still has good reason to keep and use the data held at the time of the review.

As a general rule a data review will be held every 2 years and no more than 27 calendar months after the last review. The last review took place January 2025.

Data to be reviewed

- Dundee Choral Union stores data on digital documents (e.g. spreadsheets) stored on personal devices held by committee members.
- Data stored on third party online services (e.g. Google Drive, Mail Chimp, Square)
- Physical data stored at the homes of committee members

Who the review will be conducted by

The review will be conducted by the Data Protection Officer with other committee members to be decided on at the time of the review.

How data will be deleted

- Physical data will be destroyed safely and securely, including shredding.
- All reasonable and practical efforts will be made to remove data stored digitally.

- Priority will be given to any instances where data is stored in active lists (e.g. where it could be used) and to sensitive data.
- Where deleting the data would mean deleting other data that we have a valid lawful reason to keep (e.g. on old emails) then the data may be retained safely and securely but not used.

Criteria

The following criteria will be used to make a decision about what data to keep and what to delete.

Question	Action	
	Yes	**No**
Is the data stored securely?	No action necessary	Update storage protocol in line with Data Protection policy
Does the original reason for having the data still apply?	Continue to use	Delete or remove data in accordance with Data Retention Schedule
Is the data being used for its original intention?	Continue to use	Either delete/remove in accordance with Data Retention Schedule or record lawful basis for use and get consent if necessary
Is there a statutory requirement to keep the data?	Keep the data at least until the statutory minimum no longer applies	Delete or remove the data in accordance with Data Retention Schedule unless we have reason to keep the data under other criteria.
Is the data accurate?	Continue to use	Ask the subject to confirm/update details
Where appropriate do we have consent to use the data. This consent could be implied by previous use and engagement by the individual	Continue to use	Get consent
Can the data be anonymised	Anonymise data	Continue to use

Statutory Requirements

Date stored by Dundee Choral Union may be retained based in statutory requirements for storing data other than data protection regulations. This might include but is not limited to:

- Gift Aid declarations records
- Details of payments made and received (e.g. in bank statements and accounting records)
- Trustee meeting minutes
- Contracts and agreements with suppliers/customers
- Insurance details
- Tax and employment records

Data Retention Schedule

Data Category	*Retention Period*	*Reason for Retention*	*Deletion Method*
Membership Data			
Member personal details (name, contact info)	2 years after membership ends	Allows for possible rejoining or future communication, but not indefinite retention	Secure deletion from digital records and physical copies shredded
Payment history for membership fees ("subs")	7 years	Required for financial and tax compliance	Secure digital deletion and physical copies shredded, DCU bank records maintained separately by reputable UK bank
Gift Aid declarations for membership fees ("subs")	7 years	Required for financial and tax compliance	Secure digital deletion and physical copies shredded, DCU bank records maintained separately by reputable UK bank
Member attendance records	2 years	Useful for internal statistics and event planning	Data anonymized after 2 years, original records deleted
Concert seating plans	2 years	Useful for internal statistics and event planning	Data anonymized after 2 years, original records deleted

Supplier & Contractor Data			
Contact details	2 years after role ends	Allows for future engagement if needed	Secure digital deletion and shredding
Payment records (e.g., salary, invoices)	7 years	Required for financial and tax compliance	Secure digital deletion and physical copies shredded, DCU bank records maintained separately by reputable UK bank
Marketing & Communication Data			
Mailing list (subscribers)	Until opt-out (Immediate removal)	Consent-based marketing	Secure digital deletion upon opt-out
Email interactions (event promotions, updates)	2 years	Analytical use for event planning	Secure deletion or anonymization
Ticket booking records	2 years	Audit trail for financial & security reasons	Secure deletion
Website & Online Data			
Website usage logs	information not stored		
Cookies & tracking data	information not stored		
Event & Performance Data			
Photos & video recordings	Retained indefinitely with consent, otherwise deleted upon request	For promotional use	Ensured consent-based storage
General Administrative Data			
Committee and trustee meeting minutes	7 years	Historical and governance records	Securely stored with restricted access
Incident reports (e.g., security, data breaches)	7 years	Legal & compliance purposes	Secure storage and deletion upon expiry
Other Data			
All other data	Reviewed every 2 years	As agreed by reviewers	As agreed by reviewers

Data Breach Response Plan

Purpose & Scope

This Data Breach Response Plan ensures that Dundee Choral Union (DCU) can identify, contain, assess, and respond to personal data breaches efficiently. It applies to all personal data processed by DCU, including data held by committee members, volunteers, third-party processors (e.g., MailChimp, Google Drive), and website interactions.

It forms part of Dundee Choral Union's Data Protection Policy.

What Constitutes a Data Breach?

A personal data breach is any incident that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data.

Common breach examples include:

- Loss or theft of devices (laptop, USB, mobile phone) containing personal data.
- Hacking or malware attacks on digital files.
- Accidental sharing of member/volunteer details with unauthorized persons.
- Unauthorized access by former committee members due to failure to revoke access.
- Physical security breaches, such as lost printed documents or theft.

Roles & Responsibilities

DCU Secretary

- Leads the breach response and assesses the severity.
- Reports serious breaches to the ICO (Information Commissioner's Office) within 72 hours.
- Notifies affected individuals, if required.
- Reviews and updates this plan every two years

Committee Members & Volunteers

- Immediately report suspected or confirmed breaches to the Secretary.
- Assist in containment by securing compromised systems, changing passwords, and restricting access.
- Follow incident response procedures outlined below.

Data Breach Response Steps

Step 1: Identify & Contain the Breach (Immediate action required)

- Stop further exposure (e.g., revoke access, change passwords, isolate affected systems).
- If physical documents are lost, attempt recovery immediately (e.g., check lost property, contact relevant venues).
- If an email was sent to the wrong recipient, attempt to recall it and notify the recipient not to share the data.

Step 2: Assess the Risk & Impact (Within 12 hours of breach detection)

The Secretary & Committee must determine:

- What type of data was exposed? (e.g., contact details, payment info, sensitive data)
- Who was affected? (Members, volunteers, suppliers, website users)
- What harm could occur? (Identity theft, reputational damage, financial fraud)
- Is the breach ongoing? (Has access been revoked? Are affected systems secured?)

Step 3: Notify the ICO (If required) (Within 72 hours of discovery)

Mandatory reporting: If the breach could result in a risk to individuals' rights and freedoms (e.g., exposure of financial data, ID details, sensitive member information), DCU must report it to the ICO within 72 hours.

Non-reportable breaches: If the breach is low risk (e.g., minor email mistake without sensitive data), record the incident internally but do not notify the ICO.

ICO Report Includes:

- Description of the breach (what happened, when, and how).
- Categories & number of individuals affected.
- Possible consequences of the breach.
- Actions taken to mitigate harm.

Report a breach to the ICO via: https://ico.org.uk/for-organisations/report-a-breach/

Step 4: Notify Affected Individuals (If required) (As soon as possible, ideally within 72 hours)

If the breach is likely to cause significant harm (e.g., identity theft, financial fraud, exposure of sensitive medical data), affected individuals must be informed immediately.

Notification must include:

- What happened and what data was affected.
- What DCU is doing to mitigate risk.
- Steps individuals should take (e.g., change passwords, monitor accounts).
- DCU contact details for further assistance.

Example Notification Email:

"We regret to inform you that on [date], we experienced a data security incident involving unauthorized access to our membership contact list. Your name and email address may have been affected. We have taken immediate steps to secure our systems and prevent further risk. We advise you to monitor your email for any suspicious messages. If you have any concerns, please contact [Secretary]."

Step 5: Post-Breach Review & Prevention Measures (Within 30 days of the breach)

- Conduct a root cause analysis to understand how the breach happened.
- Update security measures (e.g., review access controls, introduce two-factor authentication, train volunteers on data handling).
- Document findings in the DCU Data Breach Register (even for non-reportable breaches).
- Review and update this Data Breach Response Plan every two years.

SC017048