DATA PRIVACY NOTICE

The Essex Association of Change Ringers (EACR)

v1.4 24 May 2018

1. Your personal data – what is it?

Personal data relates to a living individual who can be identified from that data. Identification can be by the information alone or in conjunction with any other information in the data controller's possession or likely to come into such possession. The processing of personal data is governed by the General Data Protection Regulation (the "GDPR").

2. Who are we?

The Essex Association of Change Ringers is the data controller (contact details below). This means it decides how personal data is processed and for what purposes.

3. How do we process your personal data?

The Essex Association of Change Ringers complies with its obligations under the "GDPR" by keeping personal data up to date; by storing and destroying it securely; by not collecting or retaining excessive amounts of data; by protecting personal data from loss, misuse, unauthorised access and disclosure and by ensuring that appropriate technical measures are in place to protect personal data.

We use your personal data for the following purposes: -

- To enable us to provide a voluntary service promoting bells and bell ringing for the benefit of the public in Essex as specified in our rules and objects;
- To administer membership records;
- To fundraise and promote the interests of the charity;
- To manage our members and volunteers;
- To maintain our own accounts and records (including the processing of gift aid applications);
- To maintain a list of 'helpers' for the Essex Ringing Course
- To inform you of news, events, activities within the EACR and the wider bell ringing community in which you may be interested;

4. Type/classes of information processed

We process information relevant to the above reasons/purposes. This may include:

- Personal and family details only as they relate to membership records and bell-ringing activities
- Membership details (membership class, address and contact details, date of election, length of service, etc)
- Date of birth and gender (statistical analysis to give profile of the membership enabling the Association to review from time to time the benefits provided by the Personal Accident insurance policy)
- Financial, including bank account details, in respect of membership payments, donations and Gift Aid.

We also process sensitive classes of information that may include: DBS checks; physical or mental health details insofar as they may relate to safety and insurance requirements; criminal record information only as it relates to disqualification from membership under the rules or disqualification from acting as a Charity Trustee.

- Information relating to CRB/DBS checks shall only be held by the Safeguarding Officer (SO) who shall be personally responsible for its safe keeping and non-disclosure. May be discussed with Principal Officers on a need to know basis. Must be handed over to successor SO and not retained by retiring SO.
- Information relating to disqualification shall only be held by the Treasurer and other Officers on a need to know basis. Written or electronic records must be passed on to successors and not retained by retiring officers. Records must be destroyed when no longer valid.
- Information relating to CRB/DBS checks, criminal information (disqualification from Membership or Trustee) and insurance information is likely to be "Sensitive Personal Data" under the GDPR and processing be with the specific consent of the individual to which it applies and only for the reasons listed, i.e. Safeguarding (CRB/DBS checks for reasons allowed by law); disqualification of membership as a trustee; or in relation to conditions or limitations of Insurance cover.

5. Who the information is processed about

We process personal information about:

- Members and volunteers
- Trustees
- Complainants, supporters
- Enquirers
- Advisers and representatives of other like-minded organisations

6. Legal Bases

The GDPR stipulates that personal data can be processed on one of six lawful bases: Consent, Contract, Legal obligation, Vital interests, Public task & Legitimate interests. The basis chosen depends on the data and its purpose. The Association considers that the data processed is on one of three bases: The membership and tower contact data is processed on the basis of Legitimate interest under article 6 paragraph 1(f) of the GDPR. That is, we use that data we hold in ways that people would reasonably expect; consistent with being members of the Association or a Tower Correspondent. The data collected and processed to enable reclaiming of tax paid under the Gift Aid scheme is on the basis of Legal Obligation under article 6 paragraph 1(c) of the GDPR. This means we are legally obliged to keep the data for a period of time after making a claim or until the declaration is cancelled. Personal data related to contacting the individual including but not limited to, telephone numbers and email addresses are processed on the basis of Consent under article 6 paragraph 1(a) of the GDPR. That is the information is collected by the individual requesting to be placed on a list; there is no requirement to provide any such contact information to be a member. In order to justify the use of the legitimate basis it is necessary to conduct a Legitimate Interest Assessment (LIA) and record the results. This has been devised by the UK Information Commissioner's Office (ICO) in the form of a checklist. The checklist and answers for the Association are reproduced below.

Legitimate Interest Assessment Checklist

The first part of the LIA identifies the legitimate interests:

- Why do you want to process the data; what are you trying to achieve?

To maintain communication within the organisation, to administer gift aid tax claims and tower affiliations, to assist potential visiting ringers in planning their trip.

- Who benefits from the processing? In what way?

  Members from information about the Association's activities. Visitors from being able to visit towers. The Association in reclaiming tax and receiving affiliation fees for funding its charitable activities.

- Are there any wider public benefits to the processing?

  It enables the Association to fulfil its charitable objectives more efficiently.

- How important are those benefits?

  They allow the Association to efficiently pursue its aims, objectives and public benefits at minimal cost to members and non-members alike.

- What would the impact be if you couldn't go ahead?

  Communication between the Association and its members would be severely limited. Visiting ringers would be unable to plan visits. Gift Aid tax reclaims would be more time consuming or even impossible if paper records could not be used either.

- Would your use of the data be unethical or unlawful in any way?

  No. It will be used solely for the purposes stated.

The second part deals with necessity of processing the data:

- Does this processing actually help to further that interest?

  Yes.

- Is it a reasonable way to go about it?

  It is considered the minimum necessary to achieve the desired results.

- Is there another less intrusive way to achieve the same result?

  No.

Finally, the third part is a balancing test to consider the impact of the processing:

- What is the nature of your relationship with the individual?

  They are members of the Association or potential visitors to the Association's area.

- Is any of the data particularly sensitive or private?

  No.

- Would people expect you to use their data in this way?

  Yes.

- Are you happy to explain it to them?

  Yes.

- Are some people likely to object or find it intrusive?

  We think it very unlikely as no one ever has before.

- What is the possible impact on the individual?

  Almost zero. It is expected that the processing will make the Association more efficient in dealing with both members and non-members.

- How big an impact might it have on them?

Very little.

- Are you processing children's data?
  Yes, but only to note they are paying a reduced subscription.
- Are any of the individuals vulnerable in any other way?
  We do not identify vulnerable individuals.
- Can you adopt any safeguards to minimise the impact?
  We adopt normal security precautions to minimise impact.
- Can you offer an opt-out?
  Yes.

7. Documentation

The GDPR requires that organisations document their use and location of data. The following table shows what data the Association holds and where. It also defines how long the data should be retained after use and what considerations need to be given to maintaining data security.

Location of data	Purpose of processing	Categories of individuals	Categories of personal data	Retention policy	Security considerations
Report Editor	Communication, compilation of Annual Report	District Officers, Tower correspondents	Postal address, telephone number, email address	Until replaced	Secure storage
Treasurer	Gift Aid declarations	Members	Postal address	In accordance with accounting rules	
Treasurer	Membership Forms, Membership Information Forms, tower affiliations	Members	Postal address, telephone number, email address and date of birth	Until replaced	
Treasurer	Personal accident and public liability insurance	Members	Data relating to health	Seven years. In the case of treatment to minors, it is advisable that records should be kept or at least 7 years	

				after they reach the age of majority (18)	
Secretary	Communication	District Officers	Email address	Until replaced	
District Officers	Communication	Tower correspondents, Members	Email address, telephone number	Until replaced, cease to be members or ask for removal	
Webmaster	Communication	Members	Email address	Until replaced	
Safeguarding Officer	CRB/DBS checks	Members	Postal address, telephone number and date of birth	Until replaced	
Youth Coordinator	Communication, Permission to Ring Forms	Members	Email address, date of birth and data relating to health	Until replaced	
Essex Course Administrator / Education Officer / Training Day Organisers	Process applications	Members	Postal address, email address, telephone number and data relating to health	Until after event	Secure destruction of sensitive personal data

8. Sharing your personal data

We sometimes need to share the personal information we process with the individual themselves and also with other organisations. Where this is necessary we are required to comply with all aspects of the GDPR. What follows is a description of the types of organisations we may need to share some of the personal information we process with for one or more reasons. Where necessary or required we share information with:

- Members
- Family, associates or representatives of the person whose personal data we are processing
- People who are enquiring about bell-ringing within the Association's boundaries
- Educators and examining bodies in the field of Bell Ringing
- Financial organisations relating to banking and insurance of the Association and its members
- Record Keepers in respect of Peals and Quarter Peals which relates to data published in Association Annual Reports and Minute Books, on-line (e.g. BellBoard, Pealbase, The Ringing World) and in printed publications

- Other voluntary and charitable organisations of a similar nature to the EACR

9. Transferring information overseas

We may occasionally need to transfer personal information overseas but only for people who may be listed as Tower Correspondents. Where this is necessary this may be to countries or territories around the world. We are required to ensure that when we need to do this we comply with the GDPR.

10. How long do we keep your personal data?

We keep data in accordance with the guidance set out in the Charity Commission and HMRC guidance. Specifically, we retain membership data while it is still current; accounting records - these records (e.g. cash books, invoices, receipts, Gift Aid declarations and associated paperwork etc) must be retained until 6 years after the end of the accounting period they relate to. Minute books recording elections and Annual Reports listing members will be permanently kept. Peal and quarter peal records are considered to be public information and not personal data under the GDPR. Data relating to CRB/DBS checks, criminal information (disqualification from Membership or Trustee) and insurance information should be reviewed annually and destroyed if no longer relevant.

11. Your rights and your personal data

Unless subject to an exemption under the GDPR, you have the following rights with respect to your personal data: -

- The right to request a copy of your personal data which the Essex Association of Change Ringers holds about you;
- The right to request that the Essex Association of Change Ringers corrects any personal data if it is found to be inaccurate or out of date;
- The right to request your personal data is erased where it is no longer necessary for the Essex Association of Change Ringers to retain such data;
- The right to withdraw your consent to the processing at any time;
- The right to request that the data controller provide the data subject with his/her personal data and where possible, to transmit that data directly to another data controller, (known as the right to data portability), (where applicable) [*Only applies where the processing is based on consent or is necessary for the performance of a contract with the data subject and in either case the data controller processes the data by automated means*];
- The right, where there is a dispute in relation to the accuracy or processing of your personal data, to request a restriction is placed on further processing;
- The right to object to the processing of personal data, (where applicable) [*Only applies where processing is based on legitimate interests (or the performance of a task in the public interest/exercise of official authority); direct marketing and processing for the purposes of scientific/historical research and statistics*];
- The right to lodge a complaint with the Information Commissioners Office.

12. Data Protection Officer

The GDPR mandates the appointment of a Data Protection Officer under certain circumstances. These are:

- when you are a public authority, or
- when you are carrying out large scale systematic monitoring of individuals, or
- when you are processing large amounts of sensitive data

None of these apply to the Association and consequently an identified Data Protection Officer is **not** required.

13. Security

Any member of the Association who is processing data for the Association must take reasonable steps to keep the data secure. At the very least this means that the computer used to store the data must have an up to date operating system and up to date virus / malware protection. If someone ceases to be an officer of the Association they **must** remove any data pertaining to the Association or its members from their computer immediately. Likewise, if the computer used to store the information is to be disposed of by sale, gift or scrapping the data on it must be erased prior to disposal; preferably using a process known as shredding. This last instruction could equally apply to any personal data which is not related to the Association but stored on the computer.

Members should be careful not to disclose Association related information to third parties in emails, on websites or in newsletters, etc. For example: If they are in the habit of sending out group emails they **must** use either the blind carbon copy (Bcc) or mailing list feature of their email program and **not** send out emails with all the email addresses visible to everyone on the list. Members should be aware that websites and other online publications such as newsletters can inadvertently disclose personal information. Social media is particularly prone to disclosure, often with little user control because the posted content belongs to the provider and therefore their use in any official capacity related to the Association is specifically **not** permitted.

14. Notification

If any member who is holding Association data suffers a personal data breach, defined as 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data' then they must inform the Data Controller, General Secretary and / or the Report Editor immediately upon discovery. The details will then be recorded. There is a requirement in GDPR that the Association inform ICO within 72 hours of detection of a data breach. Since this applies only to data lost which will cause 'significant risk to people's rights and freedoms' it is deemed unlikely the Association will need to do this.

15. Further processing

We keep our privacy policy under regular review and may update this policy at any time without notice. We will tell you that we have updated the policy by emailing you at the email address you have provided to us and/or by posting an announcement on the website. By continuing to use the website after we have emailed you or posted a notice informing you of an update, you accept the changes to this Policy.

16. Contact Details

To exercise all relevant rights, queries of complaints please in the first instance contact the Essex Association of Change Ringers Data Controller at datacontroller@eacr.org.uk.

You can contact the Information Commissioners Office 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.