Coquet River Action Group

CRAG Data Protection Policy

1. Introduction

1.1 CRAG, as a Data Controller and a Data Processor, takes the privacy and security of the personal data entrusted to us very seriously and we recognise that we have a fundamental legal responsibility to ensure our compliance with current Data Protection legislation.

1.2 We only gather and use personal data about individuals or groups that CRAG has a relationship with or may need to contact

1.3 This Policy describes how this personal data is collected, handled and stored to meet data protection standards, and to comply with the current laws and regulations that govern the processing of personal data, including:

a) the Data Protection Act 2018 (DPA 2018);

b) the UK General Data Protection Regulations (UK GDPR 2018);

c) Privacy and Electronic Communications Regulations 2003 (PECR).

2. Purpose

2.1 This Data Protection Policy helps CRAG to:

a) comply with data protection law and follow good practice;

b) protect the rights of volunteers and groups with which CRAG has a relationship;

c) protect itself from data security risks listed in 5.1 below.

3. Principles

3.1 CRAG fully supports and complies with the principles of Data Protection as laid out in current legislation. These rules apply regardless of whether data is stored electronically, on paper or in any other way.

3.2 The DPA 2018 and the UK GDPR describe how organisations, including CRAG, must collect, handle and store personal information. They are underpinned by seven important principles, which state that personal data must be:

a) processed fairly and lawfully;

b) obtained only for specific, lawful purposes;

c) adequate, relevant and not excessive;

d) accurate and kept up to date;

e) be held no longer than necessary;

f) processed in accordance with the rights of data subjects;

g) protected in appropriate ways.

4. Scope

4.1 This Policy applies to all CRAG volunteers and all people working on behalf of CRAG.

4.2 It refers to all data that CRAG holds that relates to identifiable individuals.

5. Data protection risks

5.1 This policy helps to protect CRAG from data security risks, including:

a) Operational risks – a system breach could render our applications inoperative;

b) Reputational risks – failing to approach a breach in the correct way could have negative consequences on CRAG's public image;

c) Compliance risks – in certain cases, a breach my make us non-compliant with regulatory requirements, which could mean a substantial fine;

d) Financial risks – there are also financial risks associated with the above, such as legal fees, the cost of repairs, lost assets, and other unexpected costs and complications.

5.2 This policy also helps CRAG to protect individuals from the risk of financial or reputational damage that could result from the personal data entrusted to it getting into the wrong hands, through poor security, inappropriate disclosure of information, or through it being inaccurate or insufficient.

6. Responsibilities

6.1 All CRAG Committee Volunteers (including Action Group Leaders) and anyone else who processes and uses any of the personal data entrusted to CRAG must be familiar with and follow the Data Protection principles listed above.

6.2 All CRAG Committee Volunteers have some responsibility for ensuring data is collected, stored and handled appropriately.

6.3 Data Protection will form part of the induction for new Committee Volunteers.

6.4 Each Action Group that handles personal data must ensure that it is handled and processed in line with this policy and the Data Protection principles.

6.5 All CRAG volunteers and other users of CRAG equipment or services have a responsibility to check that any personal data we hold is accurate and current, and to correct or refer for correction any changes they become aware of, e.g. change of address or errors in spelling, etc.

6.6 The Committee is ultimately responsible for ensuring that CRAG meets its legal obligations. On a day-to-day basis this is delegated to a Data Protection Officer (DPO) nominated along with other officers each year by the Committee.

6.7 The role of the Data Protection Officer includes:

a) reviewing data protection procedures and policies, in line with an agreed schedule;

b) where relevant, helping volunteers check that their systems, services and equipment used for storing data meet acceptable security standards (e.g. volunteers sending out bulk messages and e-Newsletters);

c) evaluating any third-party services the organisation is considering using to store or process data, for instance, cloud computing services;

d) approving any data protection statements attached to communications such as emails and newsletters;

e) addressing data protection queries from journalists or media outlets;

f) arranging data protection training and advice for the people covered by this policy;

g) handling data protection questions from volunteers and those covered by this policy;

h) dealing with requests from individuals to see the data CRAG holds about them (also called 'subject access requests');

i) internally investigating any breach or potential breach of personal data;

j) reporting a breach if necessary to the Information Commissioner's Office.

7. Personal data

7.1 If it is possible to identify an individual directly from the information, we are processing, then that information should be considered to be personal data. If an individual can be indirectly identified from that data in combination with other information, the data will be considered to be personal data.

7.2 Personal data CRAG uses may include name, phone number, address and e-mail address etc.

7.3 It is unlikely that CRAG will collect personal data that is defined by legislation as special category data. e.g. sex, race, politics, religion, etc.

7.4 There may be circumstances where it may be difficult to determine whether data is personal data. If this is the case, as a matter of good practice, CRAG will treat the information with care, ensure that we have a clear reason for processing the data and,in particular, ensure we hold and dispose of it securely.

8. Anonymisation of personal data

8.1 Personal data that has been rendered anonymous does not fall under the definition of personal data for the purposes of the UK GDPR and the DPA 2018 Data Protection Act.

8.2 However, this policy recognises that caution must be exercised to ensure such data has been fully anonymised to the point where it is impossible to re-identify the individuals to which the data refers using any reasonably available means.

8.3 We will not assume that Data Protection legislation no longer applies until we are completely sure full anonymisation has been achieved.

9. How we use personal data

9.1 CRAG may gather, store and use personal data in a variety of ways. We collect data:

a) when individuals register to become volunteers of CRAG, or subscribe to our e-Newsletters;

b) through our social media channels;

c) when individuals register for an event or receive a CRAG service.

9.2 We may store personal data both electronically and as hard copies. We use personal data in the following ways:

a) for volunteering purposes;

b) to keep necessary internal records;

c) to enable the use of any of the services we provide;

d) to understand needs so we can improve our services;

e) for marketing purposes;

f) to deal with enquiries and complaints.

10. Marketing and promotion

10.1 CRAG gathers personal data that may sometimes be used in marketing and promotional materials, such as press releases, posters and flyers, our Annual Report and newsletters. We may also take photographs, make videos or voice recordings as a record of our events for use in future promotional activity.

10.2 We will always seek written consent (using a suitable form) from individuals or their carers, before we use their personal data in case studies or good news stories as illustrations of our work.

10.3 At events, training sessions etc., we will always inform attendees that we may make a record in the form of digital images and sound recordings, ensuring that we also give them the ability to opt out if they prefer.

10.4 We will only make/send telephone calls, texts or emails that contain marketing information, for example on our activities, or those of like-minded organisations:

a) to those who have actively consented to receive them, either by subscribing via our website or other link, or by completing a volunteer form, or

b) in line with the Privacy and Electronic Communications Regulations 2003, where it is reasonable from the context (such as using our services) to assume that they consent, even if they have not explicitly said so. Note, we will not assume consent for individuals who could be seen to be vulnerable in any way.

10.5 CRAG does not offer direct marketing. Direct marketing means offering a service to an individual and offering a means of direct response. Further, CRAG will not make/send telephone calls, texts or emails that contain any element of direct marketing on behalf of any other organisation.

10.6 There is no restriction on sending solicited marketing – that is, marketing material that an individual has specifically requested.

11. Individual rights

11.1 This Policy recognises that the UK GDPR and the DPA 2018 provide the following rights for individuals:

a) the right to be informed;

b) the right of access;

c) the right to rectification;

d) the right to erasure;

e) the right to restrict processing;

f) the right to data portability;

g) the right to object;

h) rights in relation to automated decision making and profiling.

11.2 The right to be informed

a) CRAG aims to ensure that individuals are aware that their data is being processed, that they understand how the data is being used and know how to exercise their rights.

b) To these ends, CRAG has a Privacy Statement, setting out how data relating to individuals is used and how individuals can exercise their rights. The Privacy Policy is available on the website and can be downloaded for those who request it.

c) As required by the DPA 2018 and the UK GDPR, CRAG will ensure that its Privacy Statement is easy to access, read and understand in a way that is appropriate to the intended audience.

11.3 Other rights

a) CRAG will follow specific procedures when dealing with requests from individuals wishing to exercise their rights.

b) Requests can be made in any form. We have a legal responsibility to identify that an individual has made a request to exercise their rights and handle it accordingly.

c) The legislation stipulates strict time limits for complying with such requests, therefore all Committee Volunteers must know how to recognise and deal with such a request without delay and refer it immediately to the Data Protection Officer.

d) The Data Protection Officer will then follow the correct procedure and may seek assistance from one or more Committee Volunteers.

e) A record will be kept of all requests from individuals to exercise their rights.

12. Data accuracy

12.1 The law requires CRAG to take reasonable steps to ensure data is kept accurate and up to date. It is the responsibility of all volunteers who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

a) Data will be held in as few places as necessary. To help guard against the processing of data that has become inaccurate and out of date, volunteers should not create any unnecessary additional data sets.

b) Volunteers should take every opportunity to ensure data is updated, for instance, by confirming a member's details if they call, and updating the record with any changes.

c) CRAG will make it easy for data subjects to update the information we hold about them wherever possible.

d) Data should be updated as inaccuracies are discovered. For instance, if a member can no longer be reached on their stored telephone number, it should be removed from the database.

13. Data storage

13.1 These rules describe how and where data should be safely stored.

13.2 When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason.

13.3 When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts, by strong passwords that are never shared between volunteers.

13.4 Personal data should not be saved directly to, nor stored on, removable media (like a memory stick/flash drive, CD or DVD) except with the express agreement of the Data Protection Officer. When not in use, these devices should be kept locked securely.

13.5 All servers and computers containing personal data will be protected by approved security software and a firewall.

14. Data Breaches

14.1 Data Protection legislation imposes a duty on all organisations to report certain types of personal data breach to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach, where feasible.

14.2 If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we must also inform those individuals without undue delay.

14.3 CRAG has in place suitable physical, electronic and managerial procedures to safeguard and secure the information we collect both online and offline in order to

prevent unauthorised access or disclosure. However, despite these measures, it is still possible that a personal data breach may occur.

14.4 If a breach is detected, it is vital that we follow strict rules and procedures to investigate and report the breach. Failure to report a breach, when required to do so, can result in a fine by the Information Commissioner's Office (ICO) and claims for damages from the individuals concerned, as well as possible loss of service and substantial damage to our reputation as an organisation.

14.5 Every member of CRAG's Committee and volunteers is responsible for ensuring that any potential breach is reported.

14.6 Reports should be made in the first instance to the Data Protection Officer. It is then their responsibility to report the breach to the Information Commissioner's Office and to the individuals concerned, if required to do so.

14.7 A record of any personal data breaches must be kept, regardless of whether or not they are notifiable.

15. Revision of this data protection policy

15.1 CRAG will revise this Policy as often as may be appropriate to ensure the contents remain accurate and valid in light of changing practices and statutory requirements.

15.2 At a minimum, this Policy will be reviewed every three years.

Approved and adopted: Signature _____; Date _____

Review in 3 years: Signature _____; Date_____