Pembroke Centre

GDPR Policy

Purpose and Background

The RDA Group holds information about riders, volunteers and other people involved with our activities. The Group has a responsibility to look after this information properly, and to comply with the EU General Data Protection Regulation (GDPR). It is likely that the GDPR will continue to form the basis of our Data Protection legislation, even once the UK has left the EU, so it is fully taken into account in this policy.

Good Data Protection practice is not just a matter of legal compliance and ticking the boxes. Data Protection is about taking care of people and respecting their privacy. Poor practice or a serious breach could not only harm individuals but would also have a serious effect on the reputation of our group and RDA as a whole.

Scope

This policy applies to information relating to identifiable individuals which is held by The Pembroke Centre

Our legal basis for using people's data

Everything we do with records about individuals – obtaining the information, storing it, using it, sharing it, even deleting it – will have an acceptable legal basis. There are six of these:

- Consent from the individual (or someone authorised to consent on their behalf).
- Where it is *necessary* in connection with a contract between our group and the individual
- Where it is *necessary* because of a legal obligation – if the law says you must, you must
- Where it is *necessary* in an emergency, to protect an individual's 'vital interests'
- Where it involves the exercise of a public function – i.e. most activities of most government, local
- government and other public bodies
- Where it is *necessary* in our legitimate interests, as long as these are not outweighed by the interests of the individual

Where we are basing our processing on consent, we will be able to 'demonstrate' that we hold consent. This means having a record of who gave consent, when they gave it, how they gave it (e.g. on the website, on a form, verbally) and what they actually consented to.

In the case of legitimate interests we will do a balancing test, and be confident that our legitimate interests in using the data in a particular way – for example in providing our services or raising funds to support them – are not over-ridden by the interests of the individual.

There are additional considerations where we are holding information about people's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and also genetic data or biometric data, health data or data concerning their sex life or sexual orientation. We will legitimise the use of any of these categories of data by having the individual's *explicit* consent.

Data Protection Principles

Data Protection compliance is based largely on a set of Principles.

The six GDPR Principles say that:

- Whatever you do with people's information has to be fair and legal. This includes making sure that they know what you are doing with the information about them.
- When you obtain information you must be clear why you are obtaining it, and must then use it only for the original purpose(s).
- You must hold the right information for your purposes: it must be adequate, relevant and limited to what is necessary
- Your information must be accurate and, where necessary, up to date
- You must not hold information longer than necessary
- You must have appropriate security to prevent your information being lost, damaged, or getting into the wrong hands

Our policy sections below reflect each of these principles in a bit more detail.

Transparency and Purposes (first and second Principles)

We will make key information available to people at the time we collect information from them. This includes:

- The identity and contact details of our group and the person who is responsible for Data Protection
- The purposes we intend to use the data for and our 'legal basis' for this (see above)
- What we regard as our 'legitimate interests', if this is our basis for processing
- Any specific recipients of the data (e.g. RDAUK) or categories of recipients

Other information will be made available where relevant. This includes:

- The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period
- Details of the individual's rights, such as to request a copy of all the data held
- The right to withdraw consent if that is the legal basis for processing (but not retrospectively)
- Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data

In both cases, we will only tell people things they won't already know. When a rider joins our group they know that we will keep a record about them and their activities with us. When a volunteer comes along it's the same. We will therefore tell them anything that may not be entirely obvious to them. This could include things like:

- The fact that RDA nationally is a separate organisation and that limited data may be passed to RDA. We will reassure people that their data is anonymous when analysed on Tracker by RDA.
- Any **direct marketing** that we may want to carry out (see below), or any additional purpose(s) that we might use the data for – publicity, perhaps. ('Data' can include photos, videos, CCTV, audio recordings, etc, not just written records.)

Direct marketing

One explicit right that people have is to stop us sending them marketing material (by post, phone, email or text) if they don't want it.

When we collect information from people that might be used for marketing we will say so at the time and ask them if they are happy to hear from us. The wording will be along the lines of: "We would like to keep you up to date with information about opportunities and events within RDA, and how you can support us. Please tick here to indicate which method(s) you are happy for us to use: Mail ☐, Phone ☐, Email ☐, Text ☐"

These rules are only for marketing. They do not stop us from contacting people in whatever is the most convenient way to give them information about things they have already signed up to, or for other administrative purposes.

Data quality, record keeping and retention (third, fourth and fifth principles)

Our activities will be more effective and appropriate if we have good quality records about the people we are working for and with. GDPR insists on this. We will ensure we have the information we need, but no more (it must be adequate, relevant and limited to what is necessary) and it will be as accurate as we can make it and – where necessary – kept as up to date as possible. We will not keep it longer than necessary.

We will remind our staff and volunteers that the individual concerned has the right to see all the information recorded about them by the group. While Data Protection concerns should never prevent us from recording the information we believe we need (especially in cases relating to safeguarding or other serious misbehaviour), being over-casual, rude or injudicious in an email could easily cause a major crisis for the group, and even the wider RDA. This can be a useful discipline in deciding what to record and how to record it.

Our group will also have a clear policy on how long to keep information. We will draw up a retention schedule, taking each type of record we hold and specifying how long we normally keep it, and our justification for this. We will set up a process for ensuring that data is deleted or destroyed routinely at the appropriate time.

Security (sixth principle)

We will take good care of the information we hold, whether on computer or on paper, and make sure that we have provided guidance and training to our staff and volunteers so that they treat the information appropriately.

In particular we will think about the risks when data is 'in transit' – either on portable devices or when it is being sent out. For example:

- If people are using their personal phone, laptop, camera or other device for our group's purposes there will be clear expectations of how they should be secured.
- When sending information, particularly by email, we will take steps to prevent confidential information being sent to the wrong person. For example, by using password-protected documents and sending the password in a separate email.
- We will also take care not to disclose people's email addresses or other information inappropriately by carelessly copying in a large number of people or forwarding an email that has been copied widely.
- Information on paper will not be left lying around, and will only be taken out of a secure location when this is really necessary.
- Where information is processed for us externally (for example by RDA) we will expect the external organisation to be able to give us satisfactory guarantees about the security measures they take.

Responsibilities

Responsibility for compliance with Data Protection lies with the organisation, not with any specific individual. The Trustees as a whole body will be responsible to keep up to date with any developments, to check that we are complying and have the evidence to prove it, to give advice to staff and volunteers and to handle any issues such as a data breach or a Subject Access Request. The Trustees may designate someone to be the lead person. See Appendix 1.

We will notify RDA National Office in the event of a serious issue e.g. a data breach.

When we work in collaboration with other organisations we will sort out clearly (and in writing) who is responsible for what, in order that there are no Data Protection gaps.

If we engage external suppliers to handle data for us in any way, our contract will set out their responsibilities to handle data in a way that will not cause us to be in breach.

Annex A. Contact Details

Responsibility for compliance with Data Protection lies with the organisation, not with any specific individual. However, the Trustees may designate someone to lead on: keeping up to date with any developments; checking that we are complying and have the evidence to prove it; giving advice to staff and volunteers and handling any issues such as a data breach or a Subject Access Request.

All contact with regards to Data breaches or a Subject Access request should be submitted by email to:

riding.pembrokecentre@gmail.com

Annex B. Data Protection obligations for those handling data within the Pembroke Centre

1. Confidentiality Statement

1.1 When working for the Pembroke Centre you will often need to have access to confidential information which may include, for example:

- Personal information about individuals who are participants, volunteers, supporters or otherwise involved in the activities organised by the Pembroke Centre.
- Information about the internal business of the Pembroke Centre.
- Personal information about colleagues working for the Pembroke Centre.

1.2 The Pembroke Centre is committed to keeping this information confidential, in order to protect people and the Pembroke Centre itself. 'Confidential' means that all access to information must be on a need to know and properly authorised basis. You must use only the information you have been authorised to use, and for purposes that have been authorised. You should also be aware that under the Data Protection Act, unauthorised access to data about individual is a criminal offence.

1.3 You must assume that information is confidential unless you know that it is intended by the Pembroke Centre to be made public. Passing information to RDA Central or another RDA Branch does not count as making it public, but passing information to another organisation does.

1.4 You must also be particularly careful not to disclose confidential information to unauthorised people or cause a breach of security. In particular you must:

- Not compromise or seek to evade security measures, including computer passwords.
- Be particularly careful when sending information between the UK office and branches.
- Not verbally unnecessarily reveal confidential information, either with colleagues or people outside the Pembroke Centre.
- Not disclose information - especially over the telephone - unless you are sure that you know who you are disclosing it to, and that they are authorised to have it. This includes the personal contact details of individuals.

1.5 If you are in doubt about whether to disclose information or not, do not guess. Withhold the information while you check with an appropriate person (either the centre manager or administrator) whether the disclosure is appropriate.

1.6 Your confidentiality obligations continue to apply indefinitely after you have stopped working with the Pembroke Centre.

2. Remote working

2.1 In the course of the Pembroke Centre's day-to-day operation members of staff and volunteers regularly work outside the office. In the course of doing this, staff and volunteers should be aware that the same obligations to confidentiality apply and they should be particularly vigilant about protecting sensitive data. In particular:

2.1.1 When accessing potentially sensitive data (including emails) from a portable device (laptop, tablet, smart phone), staff and volunteers should take extra care to ensure that the data is not visible to third parties;

2.1.2 The security of data on portable devices when away from the office is the responsibility of the individual using the device - all such devices, when used for Pembroke Centre purposes must be password protected.

2.1.3 Staff and volunteers should not access the Pembroke Centre Box storage area from any public computer or while using a public Wi-Fi connection.

2.1.4 Data that is exported from the database (for example a report exported to Excel) must be treated in the same way as the data on the database;

- Staff and volunteers should not remove personal data about individuals from the office on a memory stick, portable hard drive or other portable memory device other than those owned and encrypted by the Pembroke Centre.
- Staff and volunteers should adhere to policies about updating information on the database, to ensure the accuracy and integrity of the data.
- All removable devices including USB sticks are to be encrypted

3. Passwords

3.1 Passwords are the principal method of maintaining security over electronically stored data. In order to maintain security, the following procedures must be adhered to:

3.1.1 Passwords must not be shared, other than the Office Manager and Data Controller.

3.1.2 Passwords shall be changed on a regular basis.

3.1.3 When a member of staff or volunteer ceases working for the Pembroke Centre, their passwords will be changed.

4. Use of the Pembroke Centre Shared Data Area (Box)

4.1 Any files downloaded from the the Pembroke Centre shared area are not password protected and are to be handled as such.

4.2 When using the shared area, the browser window is to be closed at the end of any session.

4.1 When using a Mobile device to access the shared area the App passcode feature is to be enabled.

5. Data Retention

5.1 The Pembroke Centre shall keep data about people for 3 years after they end their association with the group and for 3 years after their 18th birthday if they are under 18 when they part from the group. After this period the data shall be deleted. This includes records held on personal computers and devices.

6. Use of email

6.1 Email is an essential part of the Pembroke Centre's day-to-day operation. Many emails contain personal information and staff and volunteers should be aware of the following specific points in relation to data protection and the use of email:

6.1.1 Any device which is used remotely for Pembroke Centre emails (particularly smart phones or laptops) must be password protected.

6.1.2 Emails that contain any potentially sensitive information must be treated as confidential and care should be taken when managing, responding or forwarding such emails. Password protection is to be used for all database files and considered for any file with particularly sensitive information.

6.1.3 Staff and volunteers should be aware that emails are included in any data request made by an individual. An e-mail which denigrates a third person is therefore potentially libelous and might expose the Pembroke Centre, and yourself, to being sued for damages and all staff and volunteers should be aware of this when writing emails.

6.1.4 Staff or volunteers should not email personal details of an individual to a third party unless the third party is known to them and there is a clear operational reason for doing so, see section 7 of the Data protection policy.

6.1.5 Staff or volunteers should remain aware of the requirement not to store data that is no longer of use. To this end, "deleted “and "sent" email folders should be regularly reviewed and cleared