DATA PROTECTION POLICY
Wilton RDA

Purpose and Background
Wilton RDA (WRDA) holds information about riders, volunteers and other people involved with our activities. WRDA 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 WRDA

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 & 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 at Annex A;
- 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. RDA UK) 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.

When a rider or volunteer joins WRDA they know that we will keep a record about them and their activities with us and that.

- RDA UK is a separate organisation and that limited data may be passed to RDA UK
- Data[1] is anonymous when analysed on Tracker by RDA UK
- Agreement for direct marketing that we may want to carry out (see below), or any additional purpose(s) that we might use the data for such as publicity.

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.

[1] 'Data can include photos, videos, CCTV, audio recordings, etc, not just written records.

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.

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 event and activities 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 kept as up to date as is reasonably possible.

We ensure staff and volunteers are aware that individuals have 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),

Data held about individuals includes emails. WRDA policy on the use of Email is At Annex B

WRDA data retention policy it in the Group Privacy statement. 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.

WRDA stores all of its digital information in a cloud service which is password protected with very limited access.

The data is however processed and held on WRDA and personal devices. It is also exchanged by email between these devices. The WRDA policy for handling data outside of the cloud is at Annex B

Where information is processed for us externally (for example by RDA UK) we will require that external organisation to satisfy 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 lead person for Data protection is detailed at Annex A.

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

When we work in collaboration with other organisations we will detail, who is responsible for what, in order that there are no Data Protection gaps.

Should we engage external suppliers to handle personal data for us in any way, we will ensure that have a compliant GDPR policy.

April 2020

Annex A

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.

The individual currently designated is: Trustee IM - Michael Dixon

April 2020

Annex B. Data Protection obligations for those handling data within WRDA

1. Confidentiality Statement

1.1 When working for Wilton RDA (WRDA) 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 WRDA.
- Information about the internal business of WRDA.
- Personal information about colleagues working for WRDA.

1.2 WRDA is committed to keeping this information confidential, in order to protect people and WRDA 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 GDPR, unauthorised access to data about individuals is a criminal offence.

1.3 You must assume that information is confidential unless you know that it is intended by WRDA to be made public. Passing information to RDA UK or another RDA Branch does not count as making it public, should still be done with caution.

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:

1.4.1 Not compromise or seek to evade security measures, (including computer passwords.

1.4.2 Be particularly careful when sending information between WRDA and RDA UK.

1.4.3 Not verbally unnecessarily reveal confidential information, either with colleagues or people outside WRDA.

1.4.4 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 whether the disclosure is appropriate.

1.6 Your confidentiality obligations continue to apply indefinitely after you have stopped working with WRDA.

2 Remote working

2.1 In the course of WRDA'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 WRDA purposes must be password protected.

2.1.3 Staff and volunteers should not access the WRDA 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 WRDA.
- 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 stick 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 Data Controller and the Treasurer. These are stord in a private area on Box.

3.1.2 Passwords shall be changed on a regular basis.

3.1.3 When a member of staff or volunteer ceases working for WRDA their passwords will be changed.

4 Data Security

4.1 All team members must ensure that they:

- Do not leave people's information out on their desk
- Lock filing cabinets when the office is unattended
- Do not leave data displayed on screen (use a screensaver)
- Ensure that their PC screen cannot be seen by anyone who is not entitled to see it

- Do not leave their computer logged on and unattended
- Do not give their password to anyone, ever
- Do not disclose any personal information without the data subject's consent and verifying the enquirer (e.g. phone the police officer or the social worker back via the station or office switch board)
- Are aware that email can be a very risky means of communicating, especially in relation to personal information
- Are careful when responding to email e.g. using 'reply all' or 'send to all' or when forwarding email
- Ensure that all paper waste containing any personal or confidential information is to be destroyed.

5 Photogaphy

5.1 Information about participants and supporters will only be made public with their consent. This includes photographs. The only exception to this shall be 'public' event such as the fete and carol service where the press may be present and we will have a photographer there. Participation in the event shall be taken as permission to publish the photographs. Notices shall be displayed to that effect at the event.

6 Use of the WRDA Shared Data Area (Box)

6.1 Any files downloaded from the WRDA shared area are not password protected and are to be handled as such.

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

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

7 Use of email

7.1 Email is an essential part of WRDA'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:

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

7.1.2 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 contaning personal information and considered for any file with particularly sensitive

information.

7.1.3 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 WRDA, and yourself, to being sued for damages and all staff and volunteers should be aware of this when writing emails.

7.1.4 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.

7.1.5 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.

7.1.6 When sending emails to multiple external addressees or all volunteers or riders for example BCC is to be used where the addressees may not know each other or may not want their address shared. It is not to be used for internal emails for example to Trutees and Staff solely for privacy reasons; it is not possible to ‘reply to all’ or to see who else is included in the distribution, both key requirements to good workflow.