Royal Welsh Agricultural Society

Data Protection Policy

1. The Royal Welsh Agricultural Society, hereinafter the "Society" is the Data Controller under the General Data Protection Regulation, which means that it determines what purposes personal information held, or will be used for. It is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for.

2. The Data Controller of Society, hereinafter "DC", needs to gather and use certain information about individuals.

3. These can include clients, customers, suppliers, business contacts, employees and other people the practice has a relationship with or may need to contact.

4. This policy describes how this personal data must be collected, handled, stored to meet the practice's data protection standards – and to comply with the law. It also outlines how requests for access to the data will be treated.

5. This data protection policy exists to ensure that the Society:

5.1. Complies with Data Protection law and follows good practice

5.2. Protects the rights of staff, clients, customers and partners

5.3. Is open about how it stores and processes individual's data

5.4. Protects itself from the risks of a data breach.

6. The General Data Protection Regulation describes how organisations must collect, handle, and store personal information.

7. These rules apply regardless of whether data is stored electronically, on paper or on other materials.

8. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

9. The General Data Protection Regulation is underpinned by six important principles. They say that personal data must be:

9.1. processed **lawfully, fairly, and transparently**

9.2. collected for **specific, explicit, and legitimate purposes**

9.3. adequate, relevant, and limited to what is necessary for processing

9.4. accurate and, where necessary, kept up to date.

9.5. kept in a form such that the Data Subject can be identified only as long as is necessary for processing

9.6. processed in a manner that ensures appropriate security of the personal data

10. This policy will be updated as necessary to reflect best practice in data management, security, and control and to ensure compliance with any changes or amendments made to the General Data Protection Regulation.

11. This policy applies to:

11.1. All employees of the Society that includes management, trainees, volunteers, work experience students, placements and support staff.

11.2. All contractors, suppliers and other people working on behalf of the Society

12. It applies to all data the practice holds relating to identifiable individuals. This can include but is not limited to:

12.1. Names of individuals, postal addresses, email addresses, telephone numbers, financial data, business names, plus any other personal sensitive information relating to individuals.

12.2. Everyone who works for the Society has responsibility for ensuring data is collected, stored and handled appropriately.

13. This policy will be updated as necessary to reflect best practice in data management, security, and control and to ensure compliance with changes or amendments made to the General Data Protection regulation.

14. The Association will, through appropriate management and strict application of criteria and controls:

14.1. Observe fully conditions regarding the fair collection and use of information

14.2. Meet its legal obligations to specify the purposes for which information is used

14.3. Collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements

14.4. Ensure the quality of information used

14.5. Ensure appropriate retention and disposal of information

14.6. Ensure that the rights of people about whom information is held, can be fully exercised under the GDPR. These include:

14.6.1. The right to be informed

14.6.2. The right of access

14.6.3. The right to rectification

14.6.4. The right to erase

14.6.5. The right to restrict processing

14.6.6. The right to data portability

14.6.7. The right to object

14.6.8. Rights in relation to automated decision making and profiling.

14.7. Take appropriate technical and organisational security measures to safeguard personal information

14.8. Ensure that personal information is not transferred outside the EEA without suitable safeguards

14.9. Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information

14.10. Set out clear procedures for responding to requests for information

15. Information and records relating to service users will be stored securely and will only be accessible to authorised staff and data processors.

16. Information will be stored for only as long as it is needed or required by statute and will be disposed of appropriately.

17. The DC will ensure all personal and company data is non-recoverable from any computer system previously used by the Society which has been passed on/sold to a third party.

18. All individuals/data subjects have the right to access the information DC holds about them.

19. If an individual contacts the Society requesting information held about them a request will be made to them for photographic ID and if none of the exemptions arise, the information will be provided within one month of the request.

20. In addition, the DC will ensure that:

20.1. Everyone processing personal information understands that they are contractually responsible for following good data protection practice

20.2. Everyone processing personal information is appropriately trained to do so

20.3. Everyone processing personal information is appropriately supervised

20.4. Anybody interested in making enquiries about handling personal information knows what to do

20.5. It deals promptly and courteously with any enquiries about handling personal inform

20.6. It describes clearly how it handles personal information

20.7. It will regularly review and audit the ways it holds, manages and uses personal information

21. The DC may share data with other agencies such as government departments and other relevant parties.

22. The Individual/data subject will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows the DC to disclose data (including sensitive data) without the data subject's consent. These are:

22.1. Carrying out a legal duty or as authorised by the Secretary of State

22.2. Protecting vital interests of an individual/data subject or other person

22.3. The individual/data subject has already made the information public

22.4. Conducting any legal proceedings, obtaining legal advice or defending any legal rights

22.5. Monitoring for equal opportunities purposes – i.e. race, disability or religion

22.6. Providing a confidential service where the individual/data subject's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill individuals'/data subjects to provide consent signatures.

23. The DC will ensure that s/he and all employees are appropriately trained in Data Protection and particularly the policies of DC annually.

24. If new members of staff commence work they will be provided with data protection training as soon as is practicable

25. The DC will keep a register of all training provided to staff.

26. If a breach occurs, details will be recorded of the breach and the DC will consider what action should be taken.

27. A record will be kept of any decision making process in this regard, the Trustees of the Society and Directors of the Company will be informed in writing of any breach or loss.

28. The Society will keep a record of all devices holding information subject to the GDPR (listing IMEI numbers; location; users).

29. They will also keep records of any actual breaches or near misses so as to update training and education.

30. Staff using a mobile device will report the loss or theft of any such device immediately to the DC.

31. A CCTV system will be installed with a recording facility with a retention period of 28 days that complies with the ICO Code of Practice document