RFS
ROYAL FORESTRY SOCIETY
INSPIRING PASSION AND EXCELLENCE IN WOODLAND MANAGEMENT

Data Protection Guidelines for RFS Divisions

Introduction

On the 25th May 2018 the General Data Protection Regulation (GDPR) will come into effect replacing the current Data Protection Act

The GDPR applies throughout the EU and the UK Government has confirmed it will remain law in the UK after we leave the EU. These guidelines for RFS divisions are designed to help us ensure that we aren't breaking the law, while we go about our ordinary operations and help us reassure our supporters that their data is in safe hands.

You will have received many letters already asking you to confirm your consent to the use of your personal data. Consent is not the only way to comply with the law. The GDPR lists six equally valid ways for organisations to keep and use personal data of which consent is just one. The RFS has decided the most appropriate legal basis for us to use is the "legitimate interests' basis. This means we do not need to get consent from all our members but we have to make sure the personal data we record and use is **ONLY** used for the legitimate purposes of the RFS and we have safeguards in place to ensure it cannot be used for any other purpose.

Personal Data

Personal data is a key concept of the GDPR and means any information (hardcopy or electronic) that could be used to identify a living individual. *Personal data* can be held in the form of written records or images (*e.g.* a person's name and address held on a database or a photo where you can clearly see someone's face). We have a duty of care to ensure that our supporters' data is stored, shared and used responsibly

Who should have access to personal data?

RFS Divisional Committees need access to RFS Members' personal data to carry out their everyday operations. For example, to invite members in their division to a field meeting or event. Committees and divisional volunteers also need each other's personal data so they can keep in contact. All committee members and volunteers will need access to some personal data, at some point to enable them to carry out their various roles.

Who can you share personal data with?

The important thing to remember is people should only have access to the data that they need to carry out their role and data should only be used for the purpose it was intended. So, for example, the number of people who have the password to view a list of RFS member contact details should be restricted to only those individuals who send out communications that promote divisional activities.

When you share personal data with others in your division, you must now consider if the person you are sharing the data with needs all the information you are sending or not. If you decide that they don't, you must withhold the data or reduce the amount of data that is shared, to only that which is necessary.

We must never share our supporters' personal data outside the RFS, without the express, recorded permission of the individuals' to whom the data relates (except where we have a legally binding contract with a third party that covers 'third party data processing'). This extends to placing personal data in the public domain (for example, publishing our supporters' images or contact details on social media, on the internet or in a newsletter or journal). It also includes the accidental, unintentional or unlawful entry of personal data into the public domain. This means that leaving a hard copy of

members' contact details on a train, accidentally publishing an image on social media or an incident where data has been stolen by computer hackers (and we didn't take reasonable steps to protect the data with a password) could all be examples of non-compliance with the new law.

Here is the Personal Data we will provide you with and how often:

You will receive a full member list for your division once a quarter from HQ. This will be send via email in a password protected document (exactly the same as it is now).

At least once a month, though we will aim for every fortnight, you will receive an email with details of new and lost members to your division. These details will be sent in the body of an email marked 'Confidential'.

Upon request you will receive a list of emails for you to use for emailing visit notifications. This list is easy to cut and paste into your Bcc line. Remember, it's important that these lists are pasted into the Blind Copy (Bcc) line, rather than the Copy (Cc) line because we don't want to accidentally share our members' personal data with other members.

So what is new? It's the RFS's responsibility to make sure we've documented how we handle data. As a result, we can't send you any data from HQ until you have confirmed that you've read, understood and agree with the contents of this document. We will ask the same of anyone new coming into divisional roles. But remember, we are here to help (not to make things difficult). If you have any queries or concerns, just let us know.

How to store the personal data we send you:

Data we share with you must be stored in a private area which can only be accessed by those that need to see it, such as other committee members.

You should not make data or passwords available to anyone who does not need the data to carry out a role for the RFS.

The new members' data you receive can be added to your full spreadsheet which must remain password protected.

Never send the password for a document in the same email as the document itself.

Each time you receive a new full data spreadsheet this must replace the previous one which must be deleted from all devices on which it is stored.

Data should not be stored on external servers (where automatic backups are made).

If you need to email, print or reproduce personal data you must take adequate steps to protect that data. For example:

- Emails containing personal data should be marked 'Confidential'.
- Printouts or hard-copies should be securely stored and destroyed (shredded) immediately after use. This type of data should not be left on display (*e.g.* unattended, on a table at an event or during a woodland visit).
- Images where individuals are identifiable should not be stored, reproduced or shared in any way without the data subject's express permission.
- Always consider whether you really need the data, for example if you ask members to fill in a register is it really necessary to ask them to sign? The signature is personal data and should not be collected unless it is essential for the purpose. A register at a meeting just needs the name so collecting a signature cannot be justified under the 'legitimate interests' test in the GDPR

FAQs

Q. I have my own ways of storing, sharing and using personal data in my role within my RFS Division. I'm certain that my own procedures are compliant with the new GDPR legislation. Can I continue to use my own procedures, rather than the ones set out in this document?

A. Yes, but….. The new GDPR legislation requires that anyone who is storing, sharing or using personal data should be able to show a record of the decisions you made about that data (and why you made them) (*e.g.* If you are sharing data, what decisions did you make about who to share the data with and how did you come to the conclusion that this is lawful?). If you use procedures that are different to those outlined in this document, it will become your responsibility to keep records that demonstrate compliance with the GDPR. These records must be submitted to RFS HQ if requested.

Q. I am concerned that I could be held responsible if I make a mistake. Where does the buck stop? Is it with me?

A. The RFS will hold accountability for any mistakes or accidental data protection breach, if you follow the procedures outlined in this document. If data protection breaches are found to be the result of negligence or misconduct, the person or persons who caused the breach will be held accountable. The Information Commissioner's Office (ICO) have powers to prosecute and fine organisations and individuals for serious data breaches. But, to put this into perspective, the last individual to be fined by the ICO was fined £850 for maliciously sharing children's free school lunch data with other parents on social media (she was charged with unlawfully obtaining and disclosing personal data). This is a long way from an accidental breach concerning membership data of a small organisation like ours.

Q. I have a separate list of people that I notify about our woodland visits. Can I still use this list?

A. We shouldn't hold data on people that are not members of the RFS. If you have documented permission from the person that they want to receive information from yourself then this is fine, though you should still be password protecting any lists of personal details that you have if you are acting on behalf of the RFS. If you feel uncomfortable with this or do not have evidence of permissions you can advise your members that they can invite non-members along as a guest.

Q. I have RFS members from nearby divisions who want information about meetings in my division. Can HQ add them to the list they send me or do I have to add them to each new list sent out by HQ?

A. HQ can help. We have many members who are interested in meetings in other divisions. If you let HQ know then we can tag them to your and other divisions in the database, which means that they will appear on any label/email list that we send you.

Q. I use a local land agent to do all my mailing for me. Can I still give them the divisional membership list so they can do this?

A. As long as the person processing the data has read, understood and agreed to these guidelines then this is not a problem.

Q. I don't know how to password protect data that I have. What do I do?

A. If you are unsure about how to password your documents then please give us a call at HQ and we will talk you through it. It depends what your document is and what version you are using but we will be able to help you with this.

Q. What do I do if a member asks me to delete their data or asks me for a copy of the data on them held by the RFS?

A. If a member asks you to delete their data please first establish - do they no longer wish to receive information from your division, or do they no longer wish to receive information from the RFS? Once you know what they are requesting, please let HQ know who the member is and delete any details that you have stored on them.

If a member asks for a copy of the data held on them please ask them to call RFS HQ directly on 01295 678588.

Q. What do I have to do if I make a mistake? E.g. send out information to all my members and forget to bcc so everyone can see all the emails? What if I lose a registration list from a meeting?

A. Everybody makes mistakes. It happens. If you think that you may have made a data protection breach please contact HQ immediately. We will assess the risk and advise next steps.

Q. How do I dispose of data that I have and no longer need?

A. If the data is stored on your computer or another device and the data is password protected (as it should be) then it can just be deleted.

If you have paper copies of personal data this needs to be shredded, or sent to HQ where we can have it shredded for you.

Q. I still have questions. What should I do?

A. We are here to help. If you have questions about GDPR please contact RFS HQ on 01295 678588 or at rfshq@rfs.org.uk

April 2018