ACF Community Group
Personal Data Privacy Agreement

ACF has agreed to give you access to personal data of supporters held by ACF, for the sole purpose of supporting and advancing your ACF Community Group.
In accepting access to this personal data, you agree:

1. To only use the personal data for the purpose of communicating with supporters about upcoming ACF Community group meetings, events and activities.

2. That all communications with supporters will be compliant with the ACF Community Principles and that communications will not have content of a partisan nature and will only deal with ACF Community Group local tactics and local campaign goals agreed by ACF.

3. Any personal data may only be accessed by designated ACF Community Group members who have completed all designated ACF training and signed an ACF Personal Data Privacy Agreement. This data will not be accessed by, or shared with, other individuals or groups that do not meet the above requirements.

4. You have completed all ACF privacy training and understand the risks to the security of supporter data and understand that it is your responsibility to comply with ACF security practices and policies as advised to you from time to time.

5. You are responsible for the security of all data accessed, processed, downloaded or recorded under your charge and for all transactions performed with your unique logon ID. You will ensure your login ID and password are secure and will never give your logon ID or password to any other person.

6. You will not attempt to screenshot, download or take any type of data from the Action Centre system.

7. You will not misuse the data in any way including accessing it for your own purposes or allowing unauthorised access to it.

8. Where you are accessing the information via Action Centre or other information systems or ACF approved tools or applications, you will only log in using a personal device which you have taken all reasonable steps to ensure is secure. ACF describes a secure personal device as follows, with the following recommendations:
    a. It has up to date security software installed, such as anti-virus, anti-malware and/or firewall software with real time protection and at least weekly scans enabled
    b. It has up to date software and operating systems
    c. It only allows software from reputable app stores or media to be installed
    d. You don't use Peer to Peer file sharing software on the device
    e. You use a lock screen and require a password for your account and do not share that password
    f. You don't open email attachments from unknown sources

g. You don't use publicly accessible Wi-Fi networks (secured or unsecured)

Note: If you need assistance with the above, or would like your device checked for compliance, your ACF Organiser is available to assist you.

9. It is your responsibility to immediately report any issue that you become aware of, that may compromise the security or privacy of ACF information systems or the ACF data (including unauthorised access). Reports should be made to your ACF Organiser.

10. You understand that a breach of the obligations set out in this Agreement is significant and could cause serious damage to ACF, including legal action being taken against ACF and significant reputational damage. ACF understands that sometimes you may have acted in good faith but an unintentional breach may occur. In those circumstances, ACF will not take any further action in respect of the breach. However, if the breach is intentional or is due to negligent behaviour, you may be excluded from ACF and Community group activities.