Data protection guidance and checklist

This guidance is for everyone who needs access to personal data to undertake any tasks to support your local party. Please read the below guidance carefully then complete the checklist on p3 before starting any tasks to ensure you fully understand our data protection procedures.

Volunteers

Volunteers should be clear about their responsibilities when handling personal data. All volunteers handling personal data should read the data protection rules in this document and complete the checklist below before handling personal data, and should familiarise themselves with the data protection guidance on the Lib Dems website at www.libdems.org.uk/gdpr. Regular volunteers should aim to attend an HQ organised data protection training session either via webinar or during Conference – ask your local Data Officer for more details.

Non-member volunteers who handle personal data should sign a Volunteer Non-Disclosure Agreement (NDA) and returned to your local Data Officer. A list of activities which require an NDA can be found at: www.libdems.org.uk/dpm-volunteer-nda.

Volunteers should be able to understand and recognise when an individual is exercising their legal rights over their data and should be aware that they must pass on any data subject rights they receive to the Data Officer. Likewise, volunteers should also be able to recognise data breaches and know that a data breach should be reported to the Data Officer as soon as it is discovered. Guidance about data subject rights and data breaches can be found at: www.libdems.org.uk/dpm-breach-rights-processes – please read this page carefully.

Collecting Personal Data

A clear structure and recording system must be in place when gathering personal data. Any non-verbal material used to gather personal data including surveys, petitions and leaflets must contain a written Fair Processing Notice. Full guidance about using Fair Processing Notices and templates can be found at: www.libdems.org.uk/privacy-advice.

Equally, if you are gathering data verbally you must provide a verbal notice. When canvassing face to face a copy of the FPN (also provided through the link above) must always be offered.

It is essential that you obtain **clear** and **explicit** consent from individuals when gathering contact details including phone numbers and email addresses for the purpose of adding them to mailing lists or contacting them by these means in the future. This means that the individual must have consented to receive this **type** of contact.

For example, if an individual signs a petition and only provides consent for receiving updates about the progress of the petition via email you can only email them about the progress of the petition. They should not be added to your general mailing list as they have not explicitly consented to receiving any other type of contact from you.

Website and Social Media

Your website must be hosted by a party approved supplier. The full list of party approved suppliers can be found at: www.libdems.org.uk/dpm-supplier-approval.

Current approved website providers are Nationbuilder and Prater Raines. Admin and login details on social media accounts and websites should be restricted to the minimum possible number of Local Party Officers/member volunteers. Access should not be given to non-members under any circumstances.

Your social media pages including Twitter, Facebook and Instagram must include a brief fair processing notice with a link to the privacy policy, available at www.libdems.org.uk/privacy. You must not gather personal data about individuals from your social media pages unless you have **explicit** permission from individuals to do so. Simply joining a group or following a page is not explicit permission. More guidance on websites and social media can be found at: www.libdems.org.uk/gdpr-website-social-media.

Data Security

There should be clear procedures in place to ensure that the personal data you collect is secure. This should include provision of locked cupboards and drawers for storing hardcopy personal data and regular secure disposal of data that it is no longer needed using a crosscut shredder or an approved confidential waste disposal service. Ask your local Data Officer about your local arrangements.

Data should only be downloaded from Connect/Lighthouse/Nationbuilder if it is absolutely necessary. If it is necessary, the data must be deleted as soon as it is no longer required.

Storage of personal data on USB memory sticks is not permitted under any circumstances. Any personal data sent by electronic means must be encrypted with a password and the password must be sent using a different method to the method the data was sent. For example, if you send a spreadsheet of personal data via email you should send the password via phone/SMS. Full details about data security can be found at: www.libdems.org.uk/gdpr-data-security.

Data protection induction checklist

Please complete all the actions below before starting any tasks involving personal data.

Actions	Completed?
Getting started	
I have familiarised myself with the data protection rules and guidance at www.libdems.org.uk/gdpr	
If I am not a party member, I have signed the Non-Disclosure Agreement provided by the local party I'm volunteering for	
If I will be processing a lot of personal data in my role as an officer or volunteer, I have arranged with our local Data Officer or Chair to undertake further training with HQ	
If I am being registered as a Lighthouse, Connect or Nationbuilder user, I have been shown the system(s) and feel comfortable using them	
Collecting and processing data	
I know how to provide Fair Processing Notice to individuals whose data I am collecting over the phone or in person, both verbally and in written form where appropriate	
I know how to record when a member has given their explicit consent to be signed up to a newsletter or to receive emails, and update their preferences if they unsubscribe	
I know that I must get an individual's explicit permission before gathering their contact details from social media	
Storing and sharing data	
If I have access to electronic membership data, I know that I should only download it and save it if absolutely necessary, and delete it as soon as I've finished using it	
I know that I must not store any data on memory sticks under any circumstances	
I know that if I need to send data to someone else, I must password protect it and send the password through a different channel, e.g. by text if I'm emailing the data	
I know the location of the designated locked cupboard where I can store any printed data, and what our local arrangements are destroying data on paper (either with a crosscut shredder or through a dedicated confidential waste service)	
Handling requests and breaches	
I know what subject rights requests and data breaches are, and how to report them to data.protection@libdems.org.uk (with support from my local Data Officer where appropriate)	