Data protection guidance and checklist for Data Officers

Please read the below guidance carefully then complete the checklist below.

Data Officer

Every Local Party should have a Data Officer responsible for ensuring compliance with the party's Data Protection Rules. The Data Officer should generally be independent of the Chair and the Treasurer of the Local Party, to the extent this is possible within the Local Party size. This means that the Data Officer should have control over how personal data in the local party is used to ensure compliance with the law and data protection rules without interference or influence from other Local Party Officers.

The Data Officer is responsible for escalating subject rights requests to Lib Dems HQ and should be the first point of contact for volunteers if they have queries about handling personal data or if they receive a request from an individual who wants to exercise their legal rights over their data.

The Data Officer should attend Lib Dem data protection training either via webinar or at Conference and should also encourage others within the local party to attend training. It is important that the Data Officer receives and reads the Local Party Officer newsletter and is aware of any updates to data protection guidance.

Volunteers

Volunteers should be clear about their responsibilities when handling personal data. All volunteers handling personal data should read the data protection rules before handling personal data and should be aware that they can find data protection guidance on the Lib Dems website. Regular volunteers should aim to attend an HQ organised data protection training session either via webinar or during Conference. https://www.libdems.org.uk/recordedwebinars

Non member volunteers who handle personal data should sign a Volunteer Non-Disclosure Agreement (NDA). A list of activities which require an NDA can be found at: https://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: https://www.libdems.org.uk/dpm-breach-rights-processes

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 can be found at: https://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 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: https://www.libdems.org.uk/approved-suppliers

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. 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: https://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 is no longer needed using a crosscut shredder or an approved confidential waste disposal service.

Data should only be downloaded from Connect/Salesforce/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: https://www.libdems.org.uk/gdpr-data-security

Data Protection – checklist for Data Officers

This checklist takes you through the specific tasks you will need to do in your role as a Data Officer to ensure that your local party is compliant. You should also familiarise yourself with the Data Protection Induction Checklist, found here, https://www.libdems.org.uk/gdpr-dp-checklist which covers all the basics that other LPOs and any volunteers will need to know before starting any tasks using personal data.

Actions	Completed?
Pre-action: This checklist is designed to be completed by your Data Officer. All local parties must appoint a Data Officer to lead on data protection locally. You must then register them, either by email membership@libdems.org.uk or adding them in Lighthouse.	
Getting started as a Data Officer	
I have familiarised myself with the guidance and resources on data protection at www.libdems.org.uk/GDPR	
I have watched one of the recorded Data Protection sessions, which are on the website at https://www.libdems.org.uk/recordedwebinars	
I feel confident that I know how and when to report data breach and subject access requests to data.protection@libdems.org.uk, as explained on www.libdems.org.uk/dpm-breach-rights-processes	
I have Lighthouse Super User access and I am familiar with how to add trusted, trained new officer and volunteer users and grant appropriate permission levels, as outlined at www.libdems.org.uk/lighthouse	
Our local data protection procedures	
I have a plan in place for inducting new local party officers and volunteers by taking them through the Data Protection Induction Checklist	
I make sure all volunteers working with personal data who are not members are signing the non-disclosure agreement, which can be found at https://www.libdems.org.uk/dpm-volunteer-nda and I am keeping a record of this	
I have checked that computers and laptops owned by my local party are encrypted to disk level, as explained at https://www.libdems.org.uk/gdpr-data-security	
I've made sure that we have access to a locked cupboard for storing personal data, and have a cross cut shredder or a confidential waste removal service for destroying personal data securely	
I've checked that our local party only uses party approved suppliers to process personal data, and I know where to access the list of suppliers and request new suppliers for future, as outlined at www.libdems.org.uk/approved-suppliers	

I've checked that our website is hosted by a party approved supplier (currently Nationbuilder or Prater Raines), as outlined on www.libdems.org.uk/gdpr-website-social-media	
Collecting, storing and deleting data	
I am regularly checking that data is only downloaded where absolutely necessary, is stored then deleted promptly in accordance to our rules	
I am regularly reminding officers and volunteers that memory sticks must never be used to store personal data, and that documents with personal data must be password protected if sent externally, with the password shared through a different channel	
Our website and social media pages contain fair processing notices which include a link to the Lib Dems' privacy policy, as outlined at www.libdems.org.uk/gdpr-website-social-media	
I ensure that Fair Processing Notices are included on surveys, petitions and all other literature used by our local party to gather personal data both online and offline, as outlined at www.libdems.org.uk/privacy-advice	
I ensure that that a verbal Fair Processing Notice is provided to individuals verbally when personal data is gathered by anyone in our local party over the phone or in person, and a printed copy is offered when in person	
I have checked that everyone in our local party is receiving explicit and clear consent from individuals before adding them to a mailing list and that this consent is recorded on Lighthouse	

Name (Data Officer/Appointed LP Officer)

Date

Local Party