Data Security & Data Breaches

Our responsibility to secure and protect the data we collect, store and process

What data are we protecting?

We are protecting data and information assets that are used to store and process data.

Types of assets: paper-based/hard copy documents, computers, databases and software.

This involves all of us, at every level across the Lib Dems

3 key areas of Data Security

Key area	What that means in practice
Confidentiality Protecting our data against unauthorised access, distribution or publication.	Ask yourself… Who am I providing this data to? Do I need to give them all the data or just in part? Is the person I am sending this data to allowed to receive it?
Integrity Protecting our data against unauthorised modification, corruption or tampering.	Ask yourself… Have I accurately downloaded or uploaded the data? Do I need to check the data is accurate before using it?
Availability Protecting data against unplanned loss, destruction or availability.	This is more relevant to HQ and the systems being ready for you to use!

Practical reminder for processing data

Download

Use

Delete

Encrypt your data

- Always use Encryption
- Encrypt with Excel or Word
- Send passwords by a different method
- Choose a strong password
- Guidance can be found here:

https://www.libdems.org.uk/dpm-encryption

Keep your data organised and secure

Hard Copy Data

- Store papers in a locked drawer/cupboard
- Destroy hard copy data using a crosscut shredder
- If travelling with data, it should not be left unattended

Electronic Data

- Always password protect data you are emailing to other people
- You must **NOT** use USB sticks to store or transfer data under any circumstances
- Use Mailchimp, Nationbuilder, Prater Raines to send bulk emails, **NOT BCC**

Seek guidance from your Local Party Data Officer or data.protection@libdems.org.uk if you are unsure about securing data

Data Breaches

What is it?: A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction) by a controller or processor
- Sending personal data to an incorrect recipient
- Computing devices containing personal data being lost or stolen
- Alteration of personal data without permission
- Loss of availability of personal data

Our process to handle Data Breaches

Step 1.

Suspected Data Breach is identified.

You may wish to notify your Data Officer first so they can deal with the issue and correspond with HQ.

Actions you (your Data Officer) need to take...

Step 2.

Email data.protection@libdems.org.uk

Include as much information as you have:

Nature of the breach (summary of what happened)
Date and time of the breach
How many individuals may have been affected
The type of data involved
(emails/addresses/full names/personal information etc)

Actions the Data Protection Officer takes...

Step 3.

The Data Protection Officer will log the potential Data Breach internally and do the following:

Ask for more information if anything isn't clear

Make a decision about reporting to the ICO: this can be done via the ICO self assessment tool online or by phone

We have only 72 hours if it needs to be reported to the ICO

Final steps the Data Protection Officer takes...

Step 4.

DPO reviews the breach and offers recommendations to the Local Party as what to do next or reduce the breach happening again

Ask the Local Party to contact the individuals involved if appropriate/needed

Log all decisions and outcomes on the Data Breach Register

What circumstances do we need to report to the ICO?

When a breach occurs the DPO needs to consider the risk that the breach will have on the ***rights and freedoms of individuals.***

Two factors are considered:

1. The likelihood of the risk
2. The severity of the risk

In summary: The DPO will look at the type of personal data that has been breached, the volume of data, the ease of identifying individuals, severity of consequences, the number of individuals affected.

Therefore, not all Data Breaches need to be reported to the ICO

What do the ICO do when we report a breach?

- The DPO completes a form and reports to the ICO
- The ICO acknowledge the form and review it
- After a period of time we get a response
- They either open an investigation and ask for more information or
- Respond with a letter stating the matter is closed and offering recommendations
- The DPO will report this back to the original source of the breach

This process can take a few months.

For example we are currently waiting on the results of an investigation from a breach that took place in September 2020.

Day to day errors that cause Data Breaches

Most common error:

Incorrect use of BCC when sending group emails

Less common/rare errors:

Sending a data set/spreadsheet to the wrong person and not password protecting it

Mixed up names and addresses when sending direct mail

Top Tips

Double check!

Recipient email address: Am I sending this data to the correct person?

Group emails: Am I using BCC correctly for a small group? Play it safe and send individually or via an approved method for bulk emails

Amount of data: Do I need to send all of this data? Can I limit the data?

Secure transfer: Have I password protected the file?

Hard copy data: Shred documents no longer needed! Or file securely.

And for those of you who have had a Data Breach recently...

Thank you!

For reporting it quickly and accurately and making my job a little easier

Esther McGee - Data Protection Officer