Data Protection

Membership & Data Security Policy

Keeping information secure is not just common sense, it's the Law

Who should read this?

Officers and staff in Constituency Associations storing and sharing membership and voter information.

Volunteers receiving data in order to engage in membership contact, recruitment and retention and general campaigning activities.

Any Party information is confidential, but members' personal details are especially sensitive

This policy is a summary guide to fulfilling your responsibility to keep data secure and comply with the Data Protection Act 2018, while canvassing and liaising with Party members and the public.

The Data Protection Act says data:

- must only be used for proper purposes
- must be accurate and up to date
- must not be kept longer than necessary
- must be protected from loss or unauthorised use

Security of printed material

No printed material with confidential or personal information may be left where it could be seen by an unauthorised person. After use, it should be shredded, or returned to your Constituency Association office, which can arrange for its safe disposal. If you need a new or updated copy, ask for it.

Why? In the hands of the press, other parties or criminals, such information could be highly embarrassing or damaging. People **do** go to great effort to obtain such information, including checking your bins.

Computers, disks and USB drives

All personal data, whether on a desktop computer, laptop, CD, DVD, USB drives etc. must be fully encrypted in case of loss or theft. There are free tools available such as **VeraCrypt**. Microsoft and Apple's offerings, **Bitlocker** and **Filevault**, also work well when used correctly. It is so easy to do there is no excuse not to.

Why? Laptops can and do get stolen or lost. Loss of members' personal details into the hands of an identity thief could be catastrophic for the victims. Such loss needs to be reported to the Information Commissioner, who can fine or censure you and the Party.

Passwords

All passwords to computers, email accounts, websites and databases need to be strong. Currently, that means at least eight characters of uppercase, lowercase and numbers arranged so they are not easily guessable.

You may find that it works best to have just two or three really good passwords, which are all that are necessary if you also use a password database like KeePass, LastPass or 1Password, or a memorising system like PasswordGear.

Remember that a strong password written down and kept somewhere safe is much more secure than a weak password which is remembered. The “key” doesn’t have to be in your head, so long as it is physically secure, and someone who found it would still not guess what it was for.

Why? Hackers have all the time in the world, but it often takes only seconds to crack even very sophisticated passwords with high powered computers and clever guessing programs.

Email

Email is a lot less secure than you think. Never send confidential information by email unless it is encrypted. Confidential discussions getting into the wrong hands could cause political ramifications, and personal information going astray could cause legal liabilities.

If you use the encryption in applications such as Microsoft Excel, Word or WinZip as well as a strong password, data like membership reports will probably be safe.

But send the password by another means: call the recipient to say what the password is, or send them a text message. Putting the password in the email (or another email) is like having no encryption.

Why? (a) Hackers can read your email easily from anywhere, and (b) all of us, everyone, at some stage sends the wrong email to the wrong person. Pity the author’s family member who intended to forward him an email from someone she referred to as “crazy”, but she pressed “reply” instead of “forward”.

Membership and mailing lists

You must not feel that legitimate use of data is in any way prevented. Feel free to use mailing lists and electoral data for their proper purposes, like Association or branch business.

In practical terms, this means:

1. Lists provided are for Party business only.

   Why? Other use would breach the law.

2. Messages should be sent in a way that does not reveal the other email addresses to the whole audience. i.e. messages should be sent with the addresses in the “bcc” field, or using a bulk email sending tool, such as MailChimp or MS Office.

   Why? Disclosing everyone else’s email addresses discloses information about them unlawfully to others.

3. There must always be a message about how to stop receiving emails, e.g. “reply with the word unsubscribe” and any such requests must be passed promptly back to the office for suppression. (Don’t delete them, but add a “no email” flag).

   Why? Everyone must be given an opportunity to opt out of receiving emails.

4. Do not send messages too frequently.

   Why? Even Party supporters get email fatigue, and start calling it “spam”.

5. The list should be deleted when the task is completed, or after 3 months maximum and a new list obtained from the office for the next distribution, to ensure the branch is up-to-date with addresses.

   Why? Data should not be retained beyond the time it is needed, and it should be kept up to date.

Contact details

Data Protection Department, CCHQ,
4 Matthew Parker Street, London SW1H 9HQ

020 7984 8300

dataprotection@conservatives.com

Data Consent Agreement Form

Data is provided to you for the stated purpose only.

Any other use is specifically prohibited and may be a criminal offence.

If applicable, responses must be returned to the Constituency Association office by the specified date, and the data then deleted.

To be completed by the Constituency Association Office (Data Holder)

Association Name

Data Type ☐ Membership list ☐ Canvass Cards ☐ Voter contact list ☐ Other, stated below:

Data Purpose

Date for completion and return/destruction

Form below to be completed by Data recipient

Data Consent Agreement Form

I confirm that I am in receipt of Data for the purpose given overleaf.

I further confirm that I will comply with the Data Protection Act 2018 and the Conservative Party Membership and Data Security Policy, as either exist or may be amended.

To be completed by Data recipient

Given Name(s)

Family Name

Address

Please return your signed form to your Constituency Office (Data Holder)

Signature

Form above to be completed by Constituency Association Office (Data Holder)

Promoted by Alan Mabbutt OBE on behalf of the Conservative Party, both at 4 Matthew Parker Street, London SW1H 9HQ.

Published by Alan Mabbutt on behalf of the Conservative and Unionist Party, both at 4 Matthew Parker Street, London, SW1H 9HQ.