

Usage of Personal Data

Guidelines for Deputies

In order to enable you to fulfil your role as a Deputy, from time to time the Board of Deputies will issue Deputies with a copy of all Deputy email addresses and mobile telephone numbers, as a password protected PDF.

However, when processing any of this 'personal data' – ie sending emails or telephoning other Deputies, each Deputy is obliged to do so in accordance with the BoD's data protection policy (attached). This is because the Board of Deputies needs to comply with the UK's applicable laws and regulations.

The guidelines below have been set out to ensure you are able to do so.

1. When processing personal data (email addresses, phone numbers etc), Deputies must remember that they are acting on behalf of the BoD. Their data processing is considered the data processing of the BoD. If they violate the rules of the Privacy Policy, the BoD will be liable for this to third parties as the data processor under the GDPR.
2. The personal data of Deputies must be treated by each Deputy as confidential. It must not be shared with third parties (ie anyone outside the BoD staff, contractors, Honorary Officers and Deputies) and must only be used for purposes related to their position (in other words, to communicate with each other).
3. Additionally, Deputies must not disclose information which by its nature is, or that is identified by the Board (through its constitution, policies, rules or otherwise), as confidential and which has been acquired through their role, other than where proper authorization has been given.
4. All emails containing personal data (over and above individual's name) must only contain the personal data in a password-protected attachment – NOT the body of the email.
5. All emails containing personal data must be marked 'confidential'.
6. Personal data must be transmitted over secure networks only: transmission over unsecured networks is not permitted in any circumstances EG: when connecting to public WiFi networks.
7. Personal data should not be transmitted over WiFi if there is a wired alternative that is reasonably practicable.
8. Personal data contained in the body of an email, whether sent or received, must be copied from the body of that email and stored securely eg in password protected documents. The email itself must be permanently deleted.
9. Documents containing the personal data of other Deputies (such as the Deputy contact list) must not be printed out in hard copy. If, for some reason, it does become necessary to print out a hard copy of personal data, it must be stored securely in a locked cupboard or drawer, until no longer required, at which point it must be shredded.
10. When emails are sent to more than one Deputy, the email addresses of all recipients must be typed / pasted into the 'bcc' box and not the 'To' or 'cc' boxes. Deputies are not permitted to create distribution lists that use the name of organisation in the list / group title, without the express permission of the Honorary Officers or Chief Executive of the Board. Deputies breaching this condition may be subject to disciplinary procedures under the BoD's code of conduct.
11. Deputy email addresses must not be uploaded to a third party, eg Mailchimp. More information on the BoD's data protection policy can be found [here](#).

How to Password Protect a Document

Password protecting documents in Word:

- In Word, select File, Info, Protect Document
- Select Encrypt with password
- Enter a memorable password – without it, you won't be able to open the document again! (NB you will be asked to enter the password twice).
- Password protecting documents in Excel and PowerPoint
- In Excel or PowerPoint, select File, Info, Protect Workbook / presentation
- Select Encrypt with password
- Enter a memorable password – without it, you won't be able to open the document again! (NB you will be asked to enter the password twice)

If you have any questions regarding the contents of this document, please contact the BoD's Director of Operations – Andrew Leigh – at andrew.leigh@bod.org.uk.