

# Members' Data Protection Policy Statement



## Elected Members

Elected Members need to process personal data and private information (collectively called "data") in order to fulfil their role as elected representatives. If a Member processes data when they're performing a "corporate" role, for example as an Executive Member or as a member of a committee, the Council itself is the data controller, and processing needs to be carried out under the Council's policies and procedures. However, where a Member processes data as part of representing the residents of their Ward, the Member's the controller and therefore needs to have a policy in place to demonstrate how they'll comply with the data protection rules. When they're a controller, a Member's main objective is to use data carefully and proportionately where they need to, to fulfil their constituency role, having regard to individuals' privacy.

## As an elected Member, when I'm a data controller I'll strive to:

1. Adopt the least intrusive approach, only collecting and using data when I need to.
2. Always collect, use, store and process all data fairly and lawfully.
3. Make sure my processing of data has a proper legal basis. For ordinary data, consent from individuals usually isn't needed. If I'm acting in the public interest or in the exercise of my official role as a Member, I'll have a proper legal basis. For special category data, (formerly called sensitive personal data) such as data about someone's health, the legal basis will usually be that it's necessary for me to respond to a request from an individual constituent, or it might be necessary for certain other statutory functions or for substantial public interest reasons. I will make sure that where relevant, I follow the appropriate policy document for Members.
4. Make sure I collect data fairly and transparently, and that I provide the right information to individuals I get data from in the appropriate way. Usually, I will be able to rely on the privacy notice for Members which is displayed on the Council's website, and also where I meet my constituents.
5. Always use data in a way which is compatible with the purposes set out in the information I give individuals at the point of collection, or in the privacy notice for Members, or before further processing, or for other purposes which are legally permitted.
6. Only disclose or share data where this is legally permitted, or where I am required to do so by law. If I disclose or share data, I will only do this when I have balanced fairly the individual's privacy rights against the wider public interest. In particular, I will be careful not to disclose anyone's data inappropriately when I use social media.
7. Collect and process only the minimum relevant amount of data which is needed to meet the purpose for which I collected it.
8. Take every reasonable step to ensure that data are accurate and where necessary kept up to date, and make sure that inaccurate data are deleted or corrected without delay.
9. Make sure I don't keep data in a form which allows people to be identified for any longer than necessary, and that I don't keep data at all once the purpose for my processing is complete. Generally, for constituency matters I'll review whether I still need to keep people's special category data after I've held it for 24 months, and no data will be kept longer than my term of office, unless it's necessary for me to pass this on to my successor or to one of the other Ward Members. I'll make sure that all data will be securely destroyed, and I'll take advice from Council officers about how best to do this.

# Members' Data Protection Policy Statement



10. Make sure I process data securely, and protect against unauthorised or unlawful processing, and against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to data using appropriate technical and organisational measures. These measures will include as appropriate, the pseudonymisation and encryption of data, making sure systems and services are resilient, and that availability and access to data can be restored appropriately, and making sure there is regular testing and checking of how effective these measures are. Generally, even when I'm the data controller, I'll still process data on the Council's devices, and these are up to the proper standard. If I want to process data on my own device, then I'll ask for advice about this from Council officers.
11. Be responsible and accountable for all matters in this Policy Statement, and complete and keep safe the record of processing activities for Members.
12. Not transfer data to any country outside the EU, for example by using a web-based service where data is stored in another country, unless I've checked with Council officers that that country ensures an adequate level of privacy protection, or that I've provided appropriate safeguards.
13. Help data subjects exercise their rights, including the right of access, the right to rectify or complete data, the right to erasure (right to be forgotten), right to restriction of processing, right to data portability, right to object, and right not to be subject to a decision based solely on automated processing, including by always getting appropriate advice from Council officers about how to deal with any requests.
14. Make sure I use systems, technical or otherwise, which "build in" effectively the data protection principles above and safeguards for data subjects. Generally, I will use Council systems which do this.
15. Make sure that by default I only process data which are necessary for the particular purpose, and by default data is only accessible by those people who need to see it.
16. If I need to use someone to process data on my behalf as a data processor, I'll take advice from Council officers to make sure I use only a data processor who provides sufficient guarantees to implement appropriate technical and organisational measures to meet the requirements of data protection legislation, and ensure the rights of data subjects are protected.
17. Notify personal data breaches to the ICO, and communicate personal data breaches to data subjects as required by data protection legislation. To make sure I do this properly, I'll take advice from Council officers as soon as I think I might have lost data, or disclosed it when I shouldn't have, or when someone else might have got unauthorised access to the data I hold.