



LISS PARISH COUNCIL SUBJECT ACCESS REQUESTS POLICY

1. PURPOSE AND SCOPE

- 1.1. This Subject Access Requests Policy sets out your rights and LPC's obligations to you in detail, should you ("the data subject") request details of what Personal Data LPC holds about you.
- 1.2. This Subject Access Requests Policy is provided to you by Liss Parish Council ("LPC") which is the data controller for your data.
- 1.3. "Personal Data" any information about a living individual which allows them to be identified from that data (for example a name, photographs, videos, email address, or address). Identification can be by the personal data alone or in conjunction with any other personal data. The processing of personal data is governed by legislation relating to personal data which applies in the United Kingdom including the General Data Protection Regulation (the "GDPR"), the Data Protection Act 2018 ("DPA") and other legislation relating to personal data and rights such as the Human Rights Act 1998.
- 1.4. "Processing data" means any operation performed on Personal Data such as collection, recording and use.
- 1.5. LPC's policy relating to data protection and GDPR is set out in LPC's Privacy Policy.

2. PROCEDURE ON RECEIPT OF A SAR

Upon receipt of a Subject Access Request ("SAR") LPC will:-

- 2.1. verify whether it is controller of the data subject's personal data. If LPC is not controller, LPC will inform the data subject and refer them to the actual controller
- 2.2. verify the identity of the data subject and if needed request any further evidence on the identity of the data subject
- 2.3. verify the access request: i.e. is it sufficiently substantiated, is it clear to the data controller what personal data is requested. If not LPC will request additional information
- 2.4. verify whether requests are unfounded or excessive in particular because of their repetitive character. If the requests are unfounded or excessive LPC may refuse to act on the request or charge a reasonable fee
- 2.5. promptly acknowledge receipt of the SAR and inform the data subject of any costs involved in the processing of the SAR
- 2.6. verify whether LPC process the data requested. If LPC does not process any data, it will inform the data subject accordingly. LPC will at all times make sure the internal SAR policy is followed and progress can be monitored
- 2.7. ensure data will not be changed as a result of the SAR. Routine changes as part of the processing activities concerned are permitted..
- 2.8. verify whether the data requested also involves data on other data subjects and make sure this data is filtered before the requested data is supplied to the data subject. If such data cannot be filtered, LPC will ensure that other data subjects have consented to the supply of their data as part of the SAR.

3. RESPONDING TO A SAR

- 3.1. LPC will respond to a SAR within 30 days after receipt of the request.

- 3.2. If more time is needed to respond to complex requests an extension of another 60 days is permissible, provided that this is communicated to the data subject in a timely manner within the first month.
- 3.3. If LPC cannot provide the information requested it will inform the data subject of this without delay and at the latest within one month of receipt of the SAR.
- 3.4. If a SAR is submitted in electronic form, any personal data should preferably be provided by electronic means as well.
- 3.5. If data on the data subject is processed, LPC will make sure to include as a minimum the following information in the SAR response:-
 - 3.5.1. the purposes of processing
 - 3.5.2. the categories of personal data concerned
 - 3.5.3. the recipients or categories of recipients to whom personal data has been or will be disclosed, in particular in third countries or international organisations, including any appropriate safeguard for transfer of data, such as “Binding Corporate Rules”¹ or “EU model clauses”²
 - 3.5.4. where possible the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period
 - 3.5.5. the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing
 - 3.5.6. the right to lodge a complaint with the Information Commissioners Office (“ICO”)
 - 3.5.7. if the data has not been collected from the data subject: the source of the data
 - 3.5.8. the existence of any automated decision-making, including profiling and any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
- 3.6. LPC will provide a copy of the personal data undergoing processing.

4. REVIEW

This policy will be reviewed three years from the date of adoption by LPC.

Adopted by LPC on 10th June 2019

To be reviewed in 2022.

¹ “Binding Corporate Rules” is a global data protection policy covering the international transfer of personal data out of the European Union. It requires approval of a data protection regulator in the European Union. In most cases this will be the relevant regulator where an organisation’s headquarters are located. In the UK the relevant regulator is the Information Commissioner’s Office.

² “EU model clauses” are clauses approved by the European Union which govern the international transfer of personal data. The clauses can be between two data controllers or a data controller and a data processor.