Liss Parish Council
Data Protection and GDPR Policy

1. PURPOSE AND SCOPE

1.1. This Data Protection and GDPR Policy sets out your rights and Liss Parish Council's ("LPC") obligations to you in detail.

1.2. This Data Protection and GDPR Policy is provided to you by LPC, which is the data controller for your data, and should be read in conjunction with LPC Privacy Notice.

1.3. The processing of personal data is governed by legislation relating to personal data which applies in the United Kingdom including the UK General Data Protection Regulation (the "UK 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. "Personal Data" means 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.

1.5. "Processing data" means any operation performed on personal data such as collection, recording and use.

1.6. In the normal course of business LPC will receive personal data in connection with carrying out its statutory duties and responsibilities. This may include data on employees, councillors, contractors, partner organisations and members of the public.

1.7. LPC may process some of the following personal data where necessary to perform its tasks:

1.7.1. Names, titles, aliases and photographs.

1.7.2. Contact details such as telephone numbers, addresses and email addresses.

1.7.3. Where they are relevant to the services provided by LPC, or where you provide them to us, we may process information such as gender, age, marital status, nationality, education/work history, academic/professional qualifications, hobbies, family composition and dependents.

1.7.4. Where you pay for activities such as use of the village hall, allotments, pavilion, football pitches or recreation grounds, financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers and claim numbers.

1.8. The data LPC processes may include sensitive or other special categories of personal data such as criminal convictions, racial or ethnic origin, mental and physical health, details of injuries, medication/treatment received, political beliefs, trade union affiliation, genetic data, biometric data, data concerning sexual life or orientation. Where LPC carries out village wide surveys, such as in the Neighbourhood Plan or a particular project, the responses are anonymous and the questions are not generally asked on a topic that might be classified as sensitive.

1.9. LPC is sometimes sent a copy of the electoral roll for the Parish of Liss with updates as appropriate. The data protection issues associated with the electoral roll are the responsibility of East Hampshire District Council. LPC does not permit any third party to view the electoral roll that it holds.

1.10. All LPC paper documents are stored in the parish council office.

1.11. All computer records are stored on password protected computers or laptops with anti-virus software with "back-ups" stored remotely on hard-drives or memory sticks. Remote cloud storage may be used when suitably encrypted and secured.

2. LEGAL BASIS FOR PROCESSING DATA

2.1. Most of your personal data is processed for compliance with a legal obligation which includes the discharge of LPC's statutory functions and powers. Sometime when exercising these powers or duties it is necessary to process personal data of residents or people using LPC's services. LPC will always take into account your interests and rights.

2.2. LPC may also process personal data if it is necessary for the performance of a contract with you, or to take steps to enter into a contract. An example of this would be processing your data in connection with the use of the village hall or the acceptance of an allotment tenancy.

2.3. Where we are required by law to request your consent LPC will always do so.

2.4. LPC will implement appropriate security measures to protect your personal data. This section of the Data Protection Policy provides information about the third parties with whom LPC will share your personal data. These third parties also have an obligation to put in place appropriate security measures and will be responsible to you directly for the manner in which they process and protect your personal data. It is likely that LPC will need to share your data with some or all of the following (but only where necessary):-

2.4.1. LPC's agents, suppliers and contractors. For example, LPC may ask a commercial provider to publish or distribute newsletters on its behalf or to maintain its database software;

2.4.2. On occasion, other local authorities or not for profit bodies with which LPC is carrying out joint ventures e.g. in relation to facilities or events for the community.

2.5. LPC will keep some records permanently if legally required to do so. LPC may keep some other records for an extended period of time. For example, it is current best practice to keep financial records for a minimum period of 8 years to support HMRC audits or provide tax information. LPC may have legal obligations to retain some data in connection with its statutory obligations as a public authority. LPC is permitted to retain data in order to defend or pursue claims. In some cases the law imposes a time limit for such claims (for example 3 years for personal injury claims or 6 years for contract claims). LPC will retain some personal data for this purpose as long as it believes it is necessary to be able to defend or pursue such a claim. In general, LPC will endeavour to keep data only for as long as it needs it. This means that LPC will delete data when it is no longer needed.

3. YOUR PERSONAL DATA

3.1. Data is only used for the purpose for which it has been supplied.

3.2. Data is not passed onto a third party without the express consent of the data subject save as required or permitted by law.

3.3. LPC does not routinely share data.

3.4. LPC does not sell data.

3.5. LPC will comply with data protection law. This requires that the personal data LPC holds about you must be:

3.5.1. Used lawfully, fairly and in a transparent way.

3.5.2. Collected only for valid purposes that LPC has clearly explained to you and not used in any way that is incompatible with those purposes.
3.5.3. Relevant to the purposes LPC has told you about and limited only to those purposes.
3.5.4. Accurate and kept up to date.
3.5.5. Kept only as long as necessary for the purposes LPC has told you about.
3.5.6. Kept and destroyed securely including ensuring that appropriate technical and security measures are in place to protect your personal data to protect personal data from loss, misuse, unauthorised access and disclosure.

3.6. With your permission LPC may use your personal data for some or all of the following purposes to enable LPC to carry out it's duties and responsibilities which includes:
3.6.1. Deliver public services including to understand your needs to provide the services that you request and to understand what we can do for you and inform you of other relevant services;
3.6.2. Confirm your identity to provide some services;
3.6.3. Contact you by post, email, telephone or using social media;
3.6.4. Help us to build up a picture of how we are performing;
3.6.5. Prevent and detect fraud and corruption in the use of public funds and where necessary for the law enforcement functions;
3.6.6. Enable us to meet all legal and statutory obligations and powers including any delegated functions;
3.6.7. Carry out comprehensive safeguarding procedures (including due diligence and complaints handling) in accordance with best safeguarding practice from time to time with the aim of ensuring that all children and vulnerable person are provided with safe environments and generally as necessary to protect individuals from harm or injury;
3.6.8. Promote the interests of LPC;
3.6.9. Maintain LPC's own accounts and records;
3.6.10. Seek your views, opinions or comments;
3.6.11. Notify you of changes to LPC facilities, services, events and staff, councillors and role holders;
3.6.12. Send you communications which you have requested and that may be of interest to you. These may include information about campaigns, appeals, other new projects or initiatives;
3.6.13. Process relevant financial transactions including grants and payments for goods and services supplied to LPC
3.6.14. Allow the statistical analysis of data so LPC can plan the provision of services.
3.6.15. LPC processing may also include the use of CCTV systems for the prevention and prosecution of crime

4. YOUR RIGHTS REGARDING YOUR DATA

4.1. You have the following rights with respect to your personal data. The right to:
4.1.1. Ask LPC what information it holds on you and what it is used for;
4.1.2. Access the personal data LPC holds on you;
4.1.3. correct and update the personal data LPC holds on you;
4.1.4. have your personal data erased;
4.1.5. object to processing of your personal data or to restrict it to certain purposes only
4.1.6. data portability;
4.1.7. withdraw your consent to the processing at any time for any processing of data to which consent was obtained;
4.1.8. lodge a complaint with the Information Commissioner's Office.

4.2. When exercising any of the rights listed above, in order to process your request, LPC may need to verify your identity for your security. In such cases LPC will need you to respond with proof of your identity before you can exercise these rights.

4.3. The right to access personal data and to request a copy of the data held can be made.

4.4. You can contact the Information Commissioners Office ("ICO") on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

5. DATA BREACH

5.1. GDPR defines a personal data breach as "a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to, personal data transmitted, stored or otherwise processed".

5.1.1. Examples include:

5.1.1.1. Access by an unauthorised third party

5.1.1.2. Deliberate or accidental action (or inaction) by a controller or processor

5.1.1.3. Sending personal data to an incorrect recipient

5.1.1.4. Computing devices containing personal data being lost or stolen

5.1.1.5. Alteration of personal data without permission

5.1.1.6. Loss of availability of personal data LPC takes security of personal data seriously. Computers are password protected and hard copy files are kept in locked cabinets.

5.2. Consequences of a personal data breach: A breach of personal data may result in a loss of control of personal data, discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of personal data, damage to property or social disadvantage. Therefore a breach, depending on the circumstances of the breach, can have a range of effects on individuals.

5.3. LPC's duties to report a breach:

5.3.1. The Parish Clerk must be informed immediately when any member of the Council becomes aware of a data breach. The Parish Clerk should notify the Council's Chair of the breach.

5.3.2. If the breach is likely to result in a risk to the rights and freedoms of the individual, the breach must be reported by the Parish Clerk to the individual and the Information Commissioner's Office ("ICO") without undue delay and where feasible, not later than 72 hours after having become aware of the breach.

5.3.3. If the ICO is not informed within 72 hours, LPC via the Parish Clerk must give reasons for the delay when they report the breach.

5.3.4. When notifying the ICO of a breach the LPC must:

5.3.4.1. Describe the nature of the breach including the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned.

5.3.4.2. Communicate the name and contact details of the Data Protection Officer (when appointed).

5.3.4.3. Describe the likely consequences of the breach.

5.3.4.4. Describe the measures taken or proposed to be taken to address the personal data breach including measures to mitigate its possible adverse effects.

5.3.5 When notifying the individual(s) affected by the breach LPC must provide the individual(s) with details provided to the ICO.

5.3.6 LPC does not need to communicate with the individual(s) if the following applies:

5.3.6.1 It has implemented appropriate technical and organisational measures (e.g. encryption) so those measures have rendered the personal data unintelligible to any person not authorised to access it;

5.3.6.2 It has taken subsequent measures to ensure that the high risk of rights and freedoms of individuals is no longer likely to materialise, or;

5.3.6.3 It would involve a disproportionate effort.

5.4 Data processors duty to inform LPC: If a data processor who is processing personal data on behalf of the LPC (e.g. financial software) becomes aware of a personal data breach, it must notify the Council, via the Parish Clerk, without undue delay. It is then LPC's responsibility to inform the ICO. It is not the data processor's responsibility to notify the ICO.

5.5 Records of data breaches: All data breaches must be recorded whether or not they are reported to the data subjects involved. This record will help identify system failures and should be used as a way to improve the security of personal data.

5.5.5 The Parish Clerk will maintain a breach register setting out:

5.5.5.1 Date of breach;
5.5.5.2 Type of breach;
5.5.5.3 Numbers of individuals affected;
5.5.5.4 Date reported to ICO/Individual;
5.5.5.5 Actions taken to prevent breach recurring.

5.6. To report a data breaches to the ICO use the online system: https://ico.org.uk/for-organisations/report-a-breach

6. PROCEDURE ON RECEIPT OF A SUBJECT ACCESS REQUEST "SAR"

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

6.1.1. 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

6.1.2. verify the identity of the data subject and if needed request any further evidence on the identity of the data subject

6.1.3. 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

6.1.4. 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

6.1.5. promptly acknowledge receipt of the SAR and inform the data subject of any costs involved in the processing of the SAR

6.1.6. 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

6.1.7. ensure data will not be changed as a result of the SAR. Routine changes as part of the processing activities concerned are permitted..

6.1.8. 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.

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

6.2.1. 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.

6.2.2. 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.

6.2.3. If a SAR is submitted in electronic form, any personal data should preferably be provided by electronic means as well.

6.2.4. If data on the data subject is processed, LPC will make sure to include as a minimum the following information in the SAR response:

6.2.4.1. the purposes of processing;
6.2.4.2. the categories of personal data concerned;

6.2.4.3. 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 Standard Contractual Clauses" [2];

6.2.4.4. where possible the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period;

6.2.4.5. 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;

6.2.4.6. the right to lodge a complaint with the ICO;

6.2.4.7. if the date has not been collected from the data subject: the source of the data;

6.2.4.8. 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.

6.3. LPC will provide a copy of the personal data undergoing processing.

7. MISCELLANEOUS PROVISIONS

7.1. Any personal data transferred to countries or territories outside the UK will only be placed on systems complying with measures giving equivalent protection of personal rights through international agreements. LPC's website is accessible from overseas so on occasion some personal data (for example in a newsletter) may be accessed from overseas.

7.2. If LPC wishes to use your personal data for a new purpose, not covered by this Data Protection Policy, LPC will provide you with a Privacy Notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, LPC will seek your prior consent to the new processing.

7.3. Please contact us if you have any questions about this Data Protection Policy or the personal data LPC holds about you or to exercise all relevant rights, queries or complaints at:
The Parish Clerk, Liss Parish Council, The Council Room, Village Hall, Hill Brow Road, Liss, Hampshire, GU33 7LA; or
by email to: clerk-smith@lissparishcouncil.gov.uk

8. REVIEW

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

Adopted by LPC on 12th October 2022.

To be reviewed in 2025.

[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 Standard Contractual 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.