Lancing Parish Council

Data Protection Policy

Document Control		
Version Number	V2	
Adopted on	8 May 2019	Item 60.5
Review Date	2021	

The Parish Hall
South Street, Lancing
West Sussex, BN15 8AJ

www.lancingparishcouncil.gov.uk
admin@lancingparishcouncil.gov.uk
01903 753355

Please note that alternative formats of this document may be available upon request.

1.0 INTRODUCTION

1.1 The Council holds and processes information about employees, councillors, residents and customers, and other data subjects for administrative and commercial purposes.

1.2 When handling such information, the Council and all staff or others who process or use the information, must comply with the Data Protection principles as set out in the Data Protection Act 2018 (the Act) and the General Data Protection Regulation (GDPR).

1.3 This policy is intended to: -

a) Ensure all are aware of their responsibility regarding the Act and the GDPR.
b) Set out the basic guidelines for employees and members.
c) Provide a list of definitions to assist in the understanding of Data Protection.

2.0 DEFINITIONS

2.1 Data Subject - any living individual who is the subject of personal data held by an organisation.

2.2 Data Controller - any organisation or individual who makes decisions with regard to particular personal data. This includes decisions regarding the purposes for and the way in which personal data is processed.

2.3 Data Protection Officer - responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements.

2.4 Data Processing - any operation relating to obtaining or recording data, altering or adapting data and the disclosure or dissemination of data.

2.5 Personal Data - data relating to a living individual who can be identified from that information or from the data and other information in possession of the data controller. This information includes (but is not limited to): -

a) name
b) address
c) telephone number

2.6 Sensitive Data – this is subject to much stricter conditions of processing than personal data and includes the following: -

a) commission or alleged commission by them of any offence
b) physical or mental health or condition
c) political opinions
d) proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings
e) racial or ethnic origin
f) religious or other beliefs of a similar nature
g) sex life
h) trade union membership

2.7 Third Party - any organisation or individual other than the data subject, the data controller or its agents.

3.0 DATA PROTECTION PRINCIPLES

3.1 Data must be processed fairly and lawfully.

3.2 Data must be obtained only for specific and lawful purposes and not processed in any matter incompatible with those purposes.

3.3 Data must be relevant, adequate and not excessive for those purposes.

3.4 Data must be accurate and, where necessary, kept up to date.

3.5 Data must not be kept for longer than necessary.

3.6 Data must be processed in accordance with the rights of data subjects under the Act.

3.7 Security precautions must be in place to prevent the loss, destruction or unauthorised disclosure of the data.

3.8 Data must not be transferred outside the European Economic Area unless it can be satisfied that the country in question can provide an adequate level of security for that data.

4.0 RESPONSIBILITIES

4.1 Lancing Parish Council is the Data Controller and must ensure that any processing of personal data for which they are responsible complies with the Act.

4.2 The Data Protection Officer is GDPR-*info* Limited, who acts on behalf of the Council and is responsible for:

- assisting the Council by monitoring internal compliance, informing and advising on the Council's data protection obligations, providing advice regarding Data Protection Impact Assessments (DPIAs) and acts as a contact point for data subjects.
- is an externally appointed independent expert in data protection, who is adequately resourced, and reports accordingly to the Council.
- helping the Council demonstrate compliance and accountability.

5. STORAGE AND RETENTION OF DATA

5.1 Personal data is kept in paper-based systems and/or on a password-protected computer system.

5.2 The Council will keep different types of information for differing lengths of time, depending on legal and operational requirements. More information can be found in the Council's Document Retention Scheme.

6.0 HANDLING DATA

6.1 Manual Records

a) Filing cabinets must be locked outside of normal working hours and keys must be held securely by nominated staff.
b) All papers should be securely locked away when not in use to prevent other people from inadvertently gaining access.

6.2 Electronic Records

a) Access should be controlled by unique password with passwords changed on a regular basis.
b) Passwords and access controls should be kept secure when not in use.
c) Personal information should not be left displayed on screen when not in use.
d) Removeable files (such as USB) should be filed away securely when not in use.
e) Personal information on a lap-top computer should be locked away when not in use.

6.3 Officers of the Council

a) All staff must be aware of the Act and the GDPR and of their obligations under it.
b) Individual staff members must be aware that they may be personally liable for breaches of the Act if they act outside the authority of the data controller.
c) Refresher training will be held in relation to any changes in legislation, when there is an information security incident or at the Council's discretion. Staff requiring support, advice or guidance on any element outlined in this policy should contact the Clerk.

6.4 Members of the Council

a) All Members should be fully aware of this policy and of their duties and responsibilities under the Act and the GDPR.
b) Where holding and processing personal data about individuals in the course of undertaking Council business, Members will be covered by the Council's notification and have the same responsibilities with regard to data protection as Officers of the Council.
c) Members who process electronic personal data in an individual capacity (i.e. where they are not acting on behalf of their council) are likely to qualify as data controllers and they would individually need to notify the Information Commissioner's Office.
d) Refresher training will be held in relation to any changes in legislation, when there is an information security incident or at the Council's discretion. Members requiring support, advice or guidance on any element outlined in this policy should contact the Clerk.

7.0 SUBJECT ACCESS REQUESTS

7.1 All Subject Access Requests for information must be made through the Data Protection Officer by email to info@gdpr-info.com, by post to GDPR-*info* Ltd, First Floor Unit 1, Sheddingdean Business Park, Marchants Way, Burgess Hill, West Sussex. RH15 8QY or by telephone 01444 245415 or through the web page - https://gdpr-info.com/data-protection-contact-form/.

7.2 The data subject must identify the data that is being requested and where it is being held and this information must be shown within the request. Note that the data subject is entitled to ask for all data that Lancing Parish Council holds, without specifying that data.

7.3 The date by which the identification checks, and the specification of the data sought must be recorded; Lancing Parish Council has one month from this date to provide the requested information. There are no circumstances in which an extension to that one month will be provided, and failure to provide the requested information within that one month is a breach of the GDPR.

7.4 GDPR-*info* Ltd will ensure that the requested data is collected within the time frame. Collection will entail either:

i. Collecting the data specified by the data subject; or
ii. Searching all databases and all relevant filing systems (manual files) within Lancing Parish Council including all back up and archived files, whether computerised or manual, and including all e-mail folders and archives. The Clerk maintains a data map that identifies where all data within Lancing Parish Council is stored.

7.5 GDPR-*info* Ltd maintains a record of requests for data and of its receipt, including dates. Note that data may not be altered or destroyed in order to avoid disclosing it.

7.6 GDPR-*info* Ltd is responsible for reviewing all provided documents to identify whether any third parties are identified in it and for either excising identifying third party information from the documentation or obtaining written consent from the third party for their identity to be revealed.

7.7 If the requested data falls under one of the following exemptions, it does not have to be provided:

i. Crime prevention and detection;
ii. Negotiations with the requester;
iii. Management forecasts;
iv. Confidential references given by Lancing Parish Council (not ones given to);
v. Information used for research, historical or statistical purposes; or
vi. Information covered by legal professional privilege.

7.8 The information is provided to the data subject in electronic format unless otherwise requested and all the items provided are listed on a schedule that shows the data subject's name and the date on which the information is delivered.

8. BREACH OF POLICY

8.1 Compliance with the Act and the GDPR is the responsibility of all councillors, residents, customers and members of staff. Any deliberate or reckless breach of the policy may lead to disciplinary action and where appropriate, legal proceedings.

8.2 The Clerk, on behalf of Lancing Parish Council as the data controller, shall report any personal data breach without undue delay to the Data Protection Officer (GDPR-*info* Ltd).

8.3 If a breach is reported directly to the Data Protection Officer, GDPR-*info* Ltd will notify their contact within the data controller (the Clerk), which is recorded in the Internal Breach Register.

8.4 Notifications can be made by email to info@gdpr-info.com, by post to GDPR-*info* Ltd, First Floor Unit 1, Sheddingdean Business Park, Marchants Way, Burgess Hill, West Sussex. RH15 8QY or by telephone 01444 245415.

9. BREACH NOTIFICATION DATA CONTROLLER TO SUPERVISORY AUTHORITY

9.1 GDPR-*info* Ltd shall notify the supervisory authority [Information Commissioner's Office] without undue delay, of a personal data breach.

9.2 GDPR-*info* Ltd assesses whether the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach.

9.3 If a risk to the aforementioned is likely, GDPR-*info* Ltd shall report any personal data breach to the supervisory authority without undue delay, and where feasible not later than 72 hours. Where data breach notification to the supervisory authority is not made within 72 hours, it shall be accompanied by the reasons for the delay.

9.4 The data controller (Clerk) shall provide the following information to the supervisory authority on a Breach Notification Form:

a) A description of the nature of the breach
b) The categories of personal data affected
c) Approximate number of data subjects affected
d) Approximate number of personal data records affected
e) Name and contact details of GDPR-*info* Ltd

f) Likely consequences of the breach
g) Any measures that have been or will be taken to address the breach, including mitigation
h) The information relating to the data breach, which may be provided in phases.
i) GDPR-*info* Ltd notifies their contact within the supervisory authority, which is recorded in the Internal Breach Register
j) Notification is made by [email, phone call, etc.].
k) Confirmation of receipt of this information is made by email.

10. BREACH NOTIFICATION DATA CONTROLLER TO DATA SUBJECT

10.1 Where the personal data breach is likely to result in high risk to the rights and freedoms of the data subject Lancing Parish Council shall notify the affected data subjects without undue delay, [using this form/in accordance with GDPR-*info* Ltd's recommendations].

10.2 The notification to the data subject shall describe in clear and plain language the nature of the breach including the information specified at 9.4 above.

10.3 Appropriate measures have been taken to render the personal data unusable to any person who is not authorised to access it, such as encryption.

10.4 The controller has taken subsequent measures to ensure that the rights and freedoms of the data subjects are no longer likely to materialise.

10.5 It would require a disproportionate amount of effort. In such a scenario, there shall be a public communication or similar measure whereby the data subject is informed in an equally effective manner.

10.6 The supervisory authority may where it considers the likelihood of a personal data breach resulting in high risk require the data controller to communicate the personal data breach to the data subject.

11. COMPLAINTS

11.1 Any complaints in relation to Data protection can be made to the Information Commissioner, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

LANCING PARISH COUNCIL
BREACH NOTIFICATION FORM

Name of Data Protection Officer GDPR-*info* Ltd
First Floor Unit 1, Sheddingdean Business Park, Marchants Way, Burgess Hill, West Sussex. RH15 8QY
email: info@gdpr-info.com
telephone: 01444 245415

Reference number of incident	
Date incident detected	
Date incident occurred	
Name of incident owner	
Details of incident	
Personal/Sensitive data?	
Manual/Automated data?	
Encrypted data?	
Volume of data	
Supervisory authority notified?	
Supervisory authority notification date	
Supervisory authority notification reference	
Extra information	