GENERAL DATA PROTECTION REGULATION (GDPR)POLICY

Reviewed by LPC Meeting 17 July 2023 with amendments

1.Introduction

The Loose Parish Council *(the Council)*, known as the 'Data Controller' is fully committed to compliance with the requirement of the General Data Protection Regulation (May 2018). The Council will therefore, follow procedures which aim to ensure that all Employees, Councillors, Volunteers, Partners, Processors of information who have access to any personal data held on behalf of the Council, are fully aware of, and abide by their duties under the GDPR.

The processing of data is essential to many of the services and functions carried out by local Parish Councils. The Council recognises that compliance with the GDPR will ensure that processing of any personal data is carried out fairly, lawfully, and securely.

The Council will therefore follow procedures, and aim to ensure that any relevant training as appropriate to the role being undertaken, is implemented.

2.Scope

This policy applies to the collection and processing of all personal data held by the Council, and falling within the scope of the Regulation, it includes all formats including paper (hardcopies), electronic, audio and visual. It applies to all Employees, Councillors, Volunteers, Partners, Processors of information who have access to any personal data held on behalf of the Council.

Reference to be made to the following Loose Parish Council policy documents:

- Document Retention & Disposal Policy
- Document Retention Appx document
- Data Audit Schedule & Impact Statement
- General privacy notice- (inc on website)
- Hirers privacy notice
- Employees privacy notice
- Councillors privacy notice

3. Personal and Special Category Personal Data

The Regulation provides conditions for the collection and processing of any personal data and 'special category' personal data:

Personal Data- means any information relating to an identifiable natural person (Data Subject); an identifiable natural person is one who can be identified directly or indirectly, in particular 'by name', an 'identification number', 'location data', or 'online identifier'.

Special Category Personal Data- is defined as personal data consisting of information as to; racial or ethnic origin, political opinion, religious or other beliefs, trade union memberships, physical or mental health conditions, sexual orientation, genetics, biometric data.

4.Personal Data Processed by the Council

The Council processes personal data for many reasons, including in relation to the services it provides and as an employer. Data is processed in accordance with the GDPR and this policy. The Council will ensure that all personal information is collected, recorded and used whether it is on paper (hardcopy), computer records (electronic), or recorded under any other means.

5.Principles of Data Protection

The Council will follow the principles of good practice for processing personal data, and which are legally enforceable:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Obtained for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interests, historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purpose.
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
- Accurate and kept up to date.
- Kept in a form which permits identification of 'data subjects' for no longer than is necessary for the purposes for which the personal data is processed. Personal data maybe stored for longer periods for archiving purposes in the public interests, historical research purposes, or statistical purposes, subject to the implementation of the appropriate measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data. Including protection against accidental loss, destruction or damage using appropriate measures.
- Must have appropriate technical and organisational safeguards against unauthorised or unlawful processing.
- Must not be transferred to any country outside the EU.

6.Individual Rights

The Council recognises that access to personal data held about an individual is a fundamental right provided in the GDPR and include:

- Right to be informed
- Right of access to personal information
- Right to request rectification
- Right to request erasure
- Right to restrict processing in certain circumstances
- Right to data portability
- Right to object to processing
- Rights to automated decision making including profiling

These rights are called 'Data Subject Access Request'. The Council will ensure that all requests from individuals to access/ change their personal data are dealt with as quickly as possible and within the 30-day calendar day timescale as set out in the GDPR, and as long as the 'data subject' meets the requirements set out in this policy.

- The request to be made in writing or can be verbal
- Be accompanied by sufficient proof of identity
- Specify clearly the information required
- Make it clear where the response should be sent

If a 'data subject' is dissatisfied with the response received from the Council, then it can be dealt with through the Council's complaints procedures, if the 'data subject' continues to be dissatisfied. then he/she has the rights to go through the Information Commissioner's Office (ICO) for further investigation.

7.Legal Requirements

- Organisations, known as 'Data Processors,' who process personal data on behalf of the Council, are required to provide a written agreement to state that information will be

handled in compliance with the GDPR, and that the necessary technical and security measures are in place.

- Any sharing of personal data with external partners for the purposes of service provision must comply with all statutory requirements, and in line with Council policy and GDPR.
- The Council will follow relevant guidance issued by the ICO, and in line with their policy, for users of the CCTV surveillance equipment.
- The legal basis for this policy is the GDPR which provides the legal parameters for the processing of personal data. However, compliance with other legislation also has relevance; Data Protection Act 2018; Privacy and electronic Communications Regulations; The Freedom of Information Act 2000; Crime & Disorder Act 1998; Human Rights act 1998.

8.Data Security

The Council will process personal data in accordance with its relevant Policies/Procedures, and will ensure the security of all personal data held.

Appropriate technical and organisational measures shall be taken to protect against:

- Unauthorised access
- Unauthorised or unlawful processing
- Accidental loss, destruction or damage
- ICT & Cyber crime

9. Training

Data Protection training is crucial so that all staff understand their responsibilities relating to data protection and the use of personal data. Failure to comply with GDPR and the principles could result in harm to 'data subjects', and reputational damage.

10.Data Protection Impact Assessment

A Data Protection Impact Assessment (DPIA) is an integral part of data protection design and default. All computer systems should be subject to periodic assessments of data protection.

DPIA process helps to identify weaknesses or risks to data losses or breaches and consider action that needs to be taken to ensure compliance where such compliance has not yet been achieved.

DPIA applies to both electronic and paper (hardcopy) files/holding systems.

11. Criminal Offences

It is an offence to knowingly or recklessly obtain, disclose or procure the disclosure of personal data without the consent of the Council 'Data Controller'. It is also an offence to sell, or offer to sell, illegally obtained personal data, and this offence is extended to include retention of such data. Such actions carried out by such persons within the Council will be guilty of a criminal offence.

Where a 'Data Subject Access Request' is made, and is entitled to receive such information, it will be an offence for the 'Data Controller' (or its employees, Officers, Councillors or other persons under its control) to alter, deface, block, erase, destroy or conceal that information with the intention of preventing its exposure.

The ICO could consider fining Councils if appropriate organisational and technical measures are found not to be in place.

12. Breach of Personal Data

This procedure applies in the event of a personal data breach under 'Article 33 Notification of a personal data breach to the supervisory authority (ICO)', and 'Article 34 Communication of a personal data breach to the 'Data Subject' of the GDPR.

The GDPR draws a distinction between a 'Data Controller'(Council) and a 'Data Processor' (organisation processing data on behalf of the Council), in order to recognise that not all organisations involved in the processing of personal data have the same degree of responsibility.

- **Responsibility**

All users (whether Employees, Partners/ third-party users, Councillors, Volunteers, and Processors) are required to be aware of, and to follow this procedure in the event of a personal data breach.

- **Procedure – Breach Notification Data Processor to Data Controller**

All reports of personal data breach shall be reported to the Clerk (or Deputy Clerk) in her absence, without undue delay.

- **Procedure – Breach Notification Data Controller to Supervisory Authority (ICO)**

The Clerk shall notify the supervisory authority, Information Commissioner's Office (ICO) without undue delay, of a personal data breach.

a. The Clerk 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.

b. If a risk to the aforementioned is likely, the Clerk shall report any personal data breach to the ICO without undue delay, and where feasible not later than 72 hours. Where data breach notification to the ICO is not made within 72 hours, it shall be accompanied by the reasons for the delay.

c. The data controller (Clerk) shall provide the following information to the ICO & Parish Council: (a reporting form can be used for this purpose)

- A description of the nature of the breach
- The personal data affected
- Approximate number of data subjects affected
- Approximate number of personal data records affected
- Name and contact details of the Parish Council
- Likely consequences of the breach
- Any measures that have been or will be taken to address the breach, including mitigation
- The information relating to the data breach, which may be provided in phases.
- The Clerk notifies the contact within the ICO, which is recorded for information purposes.

- **Procedure-Breach Notification Data Controller to Data Subject**

Where the personal data breach is likely to result in high risk to the rights and freedoms of the 'data subject' the Council shall notify the affected 'data subjects' without undue delay.

a. The notification to the 'data subject' shall describe clearly the nature of the breach and relevant information.

b. To confirm that appropriate measures have been taken to render the personal data unusable to any person who is not authorised to access it.

c. To confirm that the Council 'Data Controller' has taken subsequent measures to ensure the rights and freedoms of the 'Data Subject/s' are no longer affected.

d. The ICO 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.

13. Contact Details

Kim Owen, Clerk to Loose Parish Council
Address LoosePC PO Box 634 MAIDSTONE ME17 4YR
Email – office@loose-pc.gov.uk
Telephone 07855 000156