Loughton and Great Holm Parish Council

Data Protection and the Use of Personal Data Policy

Introduction

Loughton and Great Holm Parish Council are committed to the protection of personal data and comply with our obligations under the Data Protection Act (DPA)1998 and the General Data Protection Regulation (GDPR) 2018. This document sets out our staff data protection policy to assist you in handling data correctly in carrying out your duties. Councillor's computers and phones which hold data relating to council business are also subject to this policy. Employees are not permitted to store any data on their personal pcs or phones.

This policy is not intended to be a fully comprehensive guide to the Data Protection Act and any specific data protection issues should be referred to the Parish Council for advice.

The purpose of this policy is to outline the fundamentals of the Data Protection Act 1998 and the General Data Protection Regulations 2018 so that all staff and councillors are aware of them and can identify questions or issues that must be referred to the Parish Clerk.

Definitions used in this Policy

Personal Data - is any information that can identify a living individual. This includes sensitive data (see below) and examples include names, addresses, photographs, National Insurance numbers, bank account details.

Sensitive Data - is personal data relating to an individual's racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, health, sex life, criminal proceedings or convictions.

Processing - means any operation carried out by the Parish Council or its staff on personal data e.g. collection, storage, disclosure to anyone, transfer to anyone and deletion.

The Data Protection Act covers both electronic data and data held on manual records.

The Rules of Fair Processing – Key Principles

The GDPR contains 8 principles that apply to all personal data processing. The principles state that personal data:

1. Shall be processed fairly and lawfully and shall not be processed unless consent has been obtained.
2. Shall be obtained only for one or more of the purposes specified in the Act and shall not be processed in any manner incompatible with that purpose or those purposes.
3. Shall be adequate, relevant and not excessive in relation to those purposes.
4. Shall be accurate and where necessary, kept up to date.
5. Shall not be kept for longer than is necessary.
6. Shall be processed in accordance with the rights of data subjects under the Act.
7. Shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information,
8. Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of Individuals/Service Users in relation to the processing of personal information.

Staff Responsibility

(a) Principles 1-3 - The Data Protection Act requires that personal data be processed "fairly and lawfully". Personal data will not be processed fairly and lawfully unless the individual has consented to the processing. We will mainly rely on this condition in respect of personal data requested from a member of public via a marketing activity. When requesting data, we must tell the individual what we will do with the information and ask them for their consent.

Please also refer to the Loughton and Great Holm Parish Council Privacy Policy.

Sensitive data will not be processed unless it is with explicit consent or where required for the administration of justice or legal proceedings.

(b) Principle 4 – All staff and councillors must make every effort to ensure that any personal data entered onto their computers, is recorded accurately. Staff will also be responsible for updating records as and when we receive notification from the individual/contractor/agency/or other of a change in their personal details. When we are notified of bereavement the individual's details must be deleted immediately and replaced accordingly.

(c) Principle 7 - We take security measures to safeguard personal data. This includes technical measures (e.g. password protection on the computer system) or organisational measures (e.g. door locks). The measures are designed to prevent any unauthorised access to or disclosure of personal data.

Staff and councillors must do the following:

- Laptops are password protected with secure passwords containing numbers and letters. Laptops to be locked when not in use.
- IT support contractors have remote access to our computers by permission only and when used, staff should watch to ensure that access is not permitted to confidential information.
- Computer passwords are safe and are not disclosed/passed to anyone other than a fellow employee.
- Do not disclose personal data to anyone who is not a fellow employee unless the disclosure is allowed by the Parish Clerk. This includes disclosures to the police, other clients and third parties. If in doubt, take the name and address of the person seeking the disclosure and then contact the individual concerned to seek their consent to disclose or facilitate their direct contact.
- Report all security breaches or suspected breaches.
- Always shred or incinerate any paperwork that shows personal data.
- Password protect any sensitive documents.
- Any building where council work takes place must be locked when it is empty.
- All filing cabinets should be locked at the end of the day.
- Phone calls must be made within a secure environment to protect any possible transfer of data.
- The office door must be locked when not in use.

(d) Personal Data Requests & Filing – all requests by individuals or third parties to see their own or another persons' personal data held on our electronic or manual files must be received in writing. We will respond to this request within one month, to comply with the GDPR.

If a third-party requests sensitive data on an individual, we must receive consent from the individual concerned to release that data.

If an individual requests information about themselves that contains sensitive data recorded by a third party, we must receive consent from the third party to release the data.

Complaints or Comments.

Loughton and Great Holm Parish Council tries to meet the highest standards when collecting and using personal information. For this reason, we take any complaints we receive about this very seriously. We encourage people to bring it to our attention if they think that our collection or use of information is unfair, misleading or inappropriate. We would also welcome any suggestions for improving our procedures.

If you would like to make a complaint about how your data has been handled, you can e-mail or write to:

Parish Clerk
Loughton and Great Holm Parish Council
87 Kensington Drive,
Great Holm,
Milton Keynes
MK8 9AY
parish.clerk@loughtonandgreatholm-pc.gov.uk

This policy will be reviewed and re-approved by the Parish Council every 3 years, or sooner if required due to changes in legislation, regulatory guidance, Council procedures, systems or circumstances.

Next Review Due: July 2028
Last Revised and Approved: July 2025 – (FC130/25)