Haversham-cum-Little Linford Parish Council

Data Protection and the Use of Personal Data

Introduction:

Haversham-cum-Little Linford Parish Council (HLLPC) is committed to the protection of personal data and always seeks to comply with its obligations under applicable data protection law, including the Data Protection Act 1998 (DPA) and the General Data Protection Regulation 2018 (GDPR). This document provides guidance on data handling to enable staff to undertake their role effectively. Councillors' computers and mobile phones which hold data relating to council business are also subject to this policy. Employees are not permitted to store any personal data on their personal PCs or mobile phones, except where documents are downloaded for work purposes. In this case, documents need to be deleted at the end of a session.

This procedure guide is not intended to be a fully comprehensive guide to the DPA or GDPR and any specific data protection issues should be referred to the Clerk in the first instance for advice.

The purpose of this procedure is to outline fundamentals of the DPA and GDPR so that staff and councillors are aware of them and can identify questions or issues that must be referred to the Clerk.

Definitions used:

Personal Data- any information that can identify a living individual. This includes 'Sensitive Data' (see below), names, addresses, photographs, National Insurance details, bank account details, etc.

Sensitive Data- personal data relating to an individual's racial or ethnic origin, political persuasion, religious or other beliefs, trade union membership, health, sexual persuasion, criminal proceedings or convictions

Processing- any operation carried out by HLLPC and/or its staff on Personal Data, i.e. collection, storage, disclosure to anyone, transfer to anyone and deletion. This applies to both electronic files and manual files

The Rules of Fair Processing- Key Principles

GDPR contains 6 Principles that apply to all Personal Data Processing:

1. Fair process- subject data to be processed fairly, lawfully and in a transparent manner

2. Collection- for specific, explicit, legitimate purposes and not processed further for purposes incompatible with these
3. Adequacy- data collected needs to adequate, relevant and limited to what is necessary
4. Accurate- data to be kept up to date, where possible, and accurately recorded
5. Retained- kept in a form that permits identification for no longer than is necessary for the purposes for which the data has been captured and processed
6. Security- processed to ensure adequate security including protection against unauthorised or unlawful processing and against accidental loss/damage

Staff Responsibility:

Principles 1, 2 & 3- The DPA 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 rely mainly on this condition in respect of Personal Data. When requesting data we must tell the individual what we will do with the information and ask them for their active consent, being the requirement for them to specifically confirm that the parish council is able to continue to hold data for mutually agreed purposes. This can be provided verbally and should be documented.

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

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 be responsible for updating records as and when notification of changes in Personal Data are received. When notified of bereavement the individual's details should be deleted immediately.

Principle 5- All staff must ensure that regular reviews are undertaken on information files and these are deleted where required or when the purpose for which the data has been collected has ceased.

Principle 6- We take security measures to safeguard Personal Data. This includes technical measures (e.g. password protection on computer systems) and organisational measures (e.g. secure storage for physical files). The measures are designed to prevent any unauthorised access to or disclosure of Personal Data. In particular, care must be taken to always ensure that:

- Public or unauthorised personnel are not permitted access to HLLPC files and records without supervision
- PCs are password protected with secure passwords
- PCs are locked when not in use
- Keys held by HLLPC and computer passwords are safe and are not disclosed/passed to anyone other than fellow employees and councillors

- Personal Data is not disclosed to anyone unless the disclosure is allowed by the Clerk. This includes disclosures to the police, other clients and third parties. If in doubt, seek the express consent of the party in question to the release of the information
- All security breaches or suspected breaches are reported - if significant the need to be reported to the Information Commissioner's Office within 72 hours of becoming aware of the breach
- Paperwork showing Personal Data is always shredded
- Password protection is applied to sensitive documents
- External phone calls to be made in a secure environment to avoid the risk of information regarding third parties being overheard
- Website software/plug-ins kept up to date
- Website security installed and maintained

Personal Data Requests & Filing

All requests by individuals or third parties to see their own files or another person's Personal Data held on our electronic or manual files must be received **in writing.** We will respond to any request within one month, to comply with GDPR.

If a third party requests Sensitive Data on an individual we must receive the consent of the individual to release the data.

End