Data Protection Policy and Procedures

Adopted March 2024

Haversham-cum-Little Linford Parish Council ('the Council') 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 Authorised Persons to undertake their roles effectively.

This policy and procedures are 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 Authorised Persons are aware of them and can identify questions or issues that must be referred to the Clerk.

Definitions used:

Authorised Persons – all individuals who have a legitimate right to process Personal Data within the Council. This includes employees of the Council and Councillors. Ward Councillors are also subject to this Policy where it is applicable, as well as third-party auditors.

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, religion or other beliefs, trade union membership, health, sexual persuasion, criminal proceedings or convictions.

Processing – any operation carried out by Authorised Persons on Personal Data i.e. collection, storage, disclosure to anyone, transfer to anyone and deletion. This applies to both electronic and hard copy files.

Devices – any and all computers and laptops, personal or having been issued by the Council, to which Authorised Persons have access. For the avoidance of doubt, this includes smartphones and tablets.

The Rules of Fair Processing – Key Principles:

GDPR contains 6 Principles which 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 incompatible purposes
3. Adequacy – data collected needs to be 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 or damage

Authorised Persons Responsibilities:

Principles 1, 2 and 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 their Personal Data

We rely mainly on this condition in respect of Personal Data. When requested 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 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 Authorised Persons must make every effort to ensure that any Personal Data is recorded accurately. Employees will be responsible for updating records 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 employees 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 devices) 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. Particular care must be taken to always ensure that:

- Members of the public or unauthorised persons are not permitted access to electronic or hard copy records without the approval of the Clerk. Any such access will be limited to information which is strictly necessary for the purpose and any Personal Data will be removed or redacted
- Devices are password protected with strong passwords which are at least 10 characters long and use a combination of uppercase letters, lowercase letters, numbers and symbols. Where a PIN is required, the PIN should avoid obvious number combinations, sequences or dates. A biometric password is a suitable option
- Where available two-factor authentication should be used
- Devices are locked when not in use
- Physical keys held by Authorised Persons and device passwords are safe and are not disclosed/passed to anyone other than fellow Authorised Persons
- All electronic documents to be created, stored and saved on the Council drive
- Authorised Persons are permitted to make offline synchronised copies to enable them to work on documents when not connected but once reconnected and changes synchronised, the offline copy is to be deleted

- No other local copies onto personal devices are to be made and no Council information should be held solely on a personal device
- Authorised Persons are to use only their Council-provided email addresses for any correspondence pertaining to Council business
- When sending emails to a distribution list, Personal Data (i.e. email addresses) will be blind copied unless the recipients have consented to their Personal Data being shared, for example, by having previously emailed with the other recipients copied in
- Taking care to ensure forwarded emails do not contain any Personal Data in the email chain and generally by avoiding long email chains
- Personal Data is not disclosed to anyone unless the disclosure is allowed by the Clerk. This includes disclosures to the police and other 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 breach needs to be reported to the Information Commissioner's Office within 72 hours of becoming aware of the breach. The Clerk has the authority and responsibility to report a breach to the ICO in accordance with the law and the Clerk will inform the Council of the breach as soon as possible thereafter
- Paperwork showing Personal Data is always shredded
- Password protection is applied to sensitive documents and/or drives containing sensitive documents are locked-down to a specific Authorised Person
- 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

The Council and its Authorised Persons will not under any circumstances use Personal Data for marketing purposes nor otherwise disclose or share Personal Data to third parties.

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 hard copy files must be received in writing. The Council will respond to any request within one month and a small fee will be payable. This request must be made to the Clerk by email {insert email}.

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