# Tur Langton Parish Council
# Data Management and Information Security Policy
# Adopted 26/8/22 for review May 2023

The purpose of this policy is to ensure the confidentiality, integrity and availability of data is maintained and give a framework through which effective management of data can be achieved. This policy should be read in conjunction with the council's Document Retention and Disposal Policy and Data Protection Policies.

This policy applies to all records created, received or maintained by the Parish Council in the course of carrying out its functions. A record is information recorded in any form including paper, email and documents held on a computer system. Records are defined as all those documents which facilitate the business carried out by the Parish Council and which are thereafter retained. (for a set period) to provide evidence of its transactions. The policy applies to information held by the Clerk, Councillors and former Clerks and Councillors. The person with overall responsibility for the management of records is the clerk.

The General Data Protection Regulations require that personal data should be processed in a manner that ensures appropriate security of that data, including against unauthorised or unlawful processing, accidental loss, destruction or damage.

The Parish Council will ensure that all information whether stored electronically or as paper records will be stored securely to ensure that:

- Only authorised people can access, alter, disclose or destroy personal data
- The Clerk and Councillors only act within the scope of their authority
- If personal data is accidentally lost, altered or destroyed, it can be recovered to prevent any damage or distress to the individuals concerned.

**Where should records be kept?**

**Paper Records**

- Paper records should be held in a lockable, metal filing cabinet in suspension files where possible. Most paper records are also stored electronically, (see below).
- Where a document should be retained (see Document Retention and Disposal Policy) and there is not an electronic version where possible the document should be scanned to create a backup.
- Particular care should be taken with the storage of documents where no backup electronic version exists and cannot be scanned (e.g. ledgers containing archive minutes). Solutions include storage in a fire proof box or at the Records Office.

**Electronic Records** (see also below regarding emails)

- All computers, email accounts, phones, mobile devices, external hard drives and flash drives used by the clerk or councillors should be password protected and have up to date antivirus software installed where applicable
- The clerk holds the Parish Council's laptop and external hard drive, which are password protected. The chair also holds details of the passwords.
- Records stored on the council's laptop or hard drive are backed up on two password protected, encrypted memory sticks, one held by the chair and one

by the clerk. Before each meeting the clerk ensures the information on the memory stick he / she holds is updated and swaps with the stick held by the chair to ensure there is a copy of the data held away from the clerk's office / home in case of destruction by e.g. fire

- If the laptop or hard drive are disposed of the hard drive should be destroyed to prevent the information getting into the wrong hands.
- Councillors who use a shared computer should have a separate log in for Parish Council business.

**Emails**

- Emails are as much an official document as a letter or memo. They may be disclosed in response to a Data Protection or Freedom of information request and in legal cases. Electronic messages can be legally binding, contracts can be set up via email and the Parish Council may be held liable for defamatory statements in emails. For these reasons nothing should be stated in an email that would not be stated in other forms of written communication. Emails containing inaccurate information in the form of opinion or fact about an individual or organisation may result in legal action taken against the person sending the email and anyone forwarding the email on to others.
- The clerk has a dedicated email address, which is password protected, ensuring security
- Councillors are required to use Parish Council assigned email addresses (operational following the 2019 election)
- If an email contains important information or an important decision, it should be added to the relevant file or folder.
- Most emails are about trivial matters. Out of date trivial emails or those copied to the relevant subject file should be deleted as soon as possible.
- Under the Data Protection Act personal data should be kept in a form which permits identification of data subjects for no longer than is necessary and this includes emails to/from or about people.
- Neither the clerk, nor councillors acting on behalf of the Council, will forward emails from members of the public to another member of the public or another body without permission. (see also "Sharing Information" below.)

**Sharing information and confidentiality**

- If a councillor needs to access personal data from the clerk to carry out their duties this is acceptable. They are only able to access as much information as is necessary and it should only be used for that specific purpose. They should ensure that confidential or personal data is held securely and destroyed once the matter is closed.
- Data should never be used for political reasons unless the data subjects have consented.
- The clerk or councillors will not share records containing personal or confidential data with members of the public or other external stakeholders unless the data subject gives permission otherwise or this is in accordance with the General Data Protection Regulations as outlined in the Council's Data Protection Policy / General Privacy Notice.

- When complaints or queries are raised they must remain confidential unless the complainant gives permission otherwise. When handling personal data about a person other than the complainant this must also remain confidential.