Romsley Parish Council
Data Protection Policy

1. **Introduction**

Romsley Parish Council (RPC) holds and processes information about the Clerk, councillors, residents and customers, and other data subjects for administrative and commercial purposes.

When handling such information RPC, the Clerk or others who process or use the information, must comply with the Data Protection principles as set out in the Data Protection Act 1998 (the Act) (soon to become the General Data Protection Regulations (GDPR) in May 2018.

2. **Data Protection Principles**

There are eight principles set out in the 1998 Act, which in summary state that data shall:

i. Be processed fairly and lawfully;
ii. Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with the purpose;
iii. Be adequate, relevant and not excessive for the purpose;
iv. Be accurate and up-to-date;
v. Not be kept for longer than necessary for the purpose;
vi. Be processed in accordance with the Data Subject's rights;
vii. Be kept safe from unauthorised processing; and accidental loss, damage or destruction;
viii. Not be transferred to a country outside the European Economic Area, unless that country has the equivalent levels of protection for personal data, except in specified circumstances.

3. **Definitions**

"Employees, councillors, residents and customers, and other data subjects" may include past, present and potential members of those groups.
"Other data subjects" and *"third parties"* may include contractors, suppliers, contacts, referees, friends or family members.
"Processing" refers to an action involving personal information, including obtaining, viewing, copying, amending, adding, deleting, extracting, storing, disclosing or destroying information.

"Personal data" is information about an identifiable, living individual.
"Sensitive personal data" is personal data consisting of information relating to racial or ethnic origin, political opinion, religious or other beliefs, trade union membership, physical or mental or condition, sexual orientation or criminal proceedings or convictions.
"Data Controller" is a 'person' who determines the purposes for which and the manner in which any personal data are, or are to be, processed. A 'person' as recognised in law may be an individual, organisation or body of persons.
"Data Protection Officer" is an individual working on behalf of the Data Controller with responsibility for the data protection within that organisation.

4. **Responsibilities**

RPC is the Data Councillor and must ensure that any processing of personal data for which they are responsible complies with the Act.

The Data Protection Officer is the Clerk, who acts on behalf of the Council, and is responsible for:

i. Fully observing conditions regarding the fair collection and use of information;
ii. Meeting the Council's legal obligations to specify the purposes for which information is used;
iii. Collecting and processing relevant information, only to the extent that is required to fulfil operational needs/to comply with legal requirements.
iv. Ensuring the quality of information used;
v. Applying strict checks to determine the length of time that information is held;
vi. Ensuring that the rights of the people whom information is held are able to be fully exercised under the Act;
vii. Taking appropriate technical and organisational security measures to safeguard personal information;
viii. Ensuring that personal information is not transferred abroad without suitable safeguards;
ix. Ensuring that everyone managing and handling personal information;
    a. Fully understands that they are contractually responsible for following good practice in terms of protection;
    b. Is adequately trained to do so;
    c. Are appropriately supervised.

Appendix A of this policy sets out guidelines for staff members, volunteers and councillors that process or may have access to personal data.

5. **Storage and Retention**

Personal data is kept in paper-based systems and/or on a password-protected computer system.

The council will keep different types of information for differing lengths of time, depending on legal and operational requirements.

6. **Access to Information**

Any employee, councillor, resident, customer or other data subjects have a right to:

i. Ask what personal information the Council holds;
ii. Ask what this information is used for;
iii. Be provided with a copy of the information;
iv. Be given details of the purposes for which the Council uses the information and any other persons or organisations to whom it is disclosed;
v. Ask that any incorrect data held is corrected.

If it is felt by the data subject that any personal information held is incorrect the individual may request that it be amended. The Council must advise the individual within 21 days whether or not the amendment has been made.

7. **Breach of Policy**

Compliance with the Act is the responsible of all councillors and Clerk. Any deliberate or reckless breach of the policy may lead to disciplinary action and where appropriate, legal proceedings.

Any individual who believes that the council has breached any of the requirements of the Data Protection Act 1998 (or the GDPR 2018) should raise the matter with the Clerk. Alternatively, a complaint can be made to the Information Commissioner, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 4AF.

Appendix A

Guidelines for Staff, Volunteers and Councillors

During your course of your duties with RPC, you will be dealing with information such as names/addresses/phone numbers/email addresses of members of the public. You may be told or overhear sensitive information while working for CPC.

The Data Projection Act 1998 (and the subsequent General Data Protection Regulations (GDPR) 2018) gives specific guidance on how this information should be dealt with by organisations such as Romsley Parish Council. In short, to comply with the law, personal information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

To help you meet the terms of the Data Protection Act (and GDPR 2018) while working for CPC, the following guidelines are issued. Please read them carefully and ask the Data Protection Officer (Clerk) if you are in any doubt about any of them.

Sharing of Personal Information

"Personal information" includes such details as addresses/phone numbers and health details supplied by members of the public.

Such information may be shared between staff and councillors at CPC for work purposes, but should not be given to anyone outside of the council without explicit consent from the person concerned.

If such a situation arises, please ask the Clerk for advice.

Unlawful Disclosure of Personal Information

Under the Data Protection Act you are committing a criminal offence if you disclose personal information 'knowingly or recklessly' to anyone you are not supposed to, so please be careful.

Give consideration to any conversations you are having containing personal or sensitive information that could possibly be overheard by people who should not have access to such information.

Use of files, books and other paper records

In order to prevent unauthorised access and accidental loss or damage to personal information held on paper, please take good care of the files, books and other paper records you use, and ensure that they are stored before you leave the building.

Use of Email

Please ensure that before sending emails that they contain no personal or sensitive information that the recipients should not have access to. This is a particular risk when forwarding emails or adding in new recipients to an email chain.

Disposal of Scrap Paper

Be aware that names/address/phone numbers and other information written on scrap paper are also considered to be confidential. Such notes must be shredded.