

Ickleton PC: Record of Processing Activities

Document name / title	Record of Processing Activities
Version number	V1.0
Status (draft, published or superseded)	Published
Distribution	External
Author / owner	Clerk
Date of publication	September 2025
Document type (policy, standard, procedure, guide)	Register
Security classification (confidential, internal, public)	Public

1. Introduction

A Record of Processing Activities (RoPA) is a core document required under the General Data Protection Regulation (GDPR). Its purpose is to provide a detailed log of all personal data processing activities carried out by an organisation. This log helps ensure that the organisation is compliant with data protection laws and can demonstrate transparency and accountability when processing personal data.

2. Ickleton Parish Council - Record of Processing Activities (RoPA)

Processing Activity	Nature and Purpose of Processing	Categories of Data Subjects	Types of personal data	Recipients of Data	Measures to Safeguard Data	Data retention period and destruction of data once processing complete.
Identity & Contact Information Processing	To provide council services, identify individuals, and respond to communications	Service users, residents	Names, titles, aliases, contact details (phone numbers, addresses, email addresses)	Council departments, contractors (for service provision)	Secure databases, access controls, encrypted communication channels	Until there is no longer an administrative requirement.
Financial Transaction Data Processing	To manage payments for services, activities and grant payments	Service users, residents, businesses	Bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, claim numbers	Payment processors, financial institutions, auditors	Encrypted transaction systems, secure payment gateways, audit trails	Until there is no longer an administrative requirement.

Ickleton Parish Council	Record of Processing Activities					Policies and Procedures
Monitoring Equal Opportunities Compliance	To monitor and ensure compliance with equal opportunities and employment legislation	Employees, applicants, service users	Racial/ethnic origin, religious beliefs, gender, and disability data	Councillors, Clerk and external auditors	Anonymisation, access control policies	Until there is no longer an administrative requirement.
Fraud Prevention and Detection	To identify and prevent fraudulent activities, particularly in relation to public funds	Service users, residents, suppliers	Identification details, financial transaction data, addresses	Internal audit teams, law enforcement, regulatory bodies	Regular audits, transaction monitoring tools, fraud detection systems	Until there is no longer an administrative requirement.
Legal Compliance and Statutory Obligations	To comply with legal obligations, such as processing financial records, employment data, cemetery legislation and safeguarding reports	Employees, residents, contractors, service users	Financial records, tax information, employment records, name and contact details (phone numbers, addresses, email addresses)	HMRC, regulatory bodies, law enforcement	Legal compliance checks, access control policies	Until there is no longer an administrative requirement.

For any processing involving sensitive personal data (special categories), such as health information, racial/ethnic origin, and political beliefs, the local government must ensure the processing complies with the additional safeguards and justifications set out under Article 9 of the GDPR. In this case, processing is often justified for reasons of substantial public interest or legal obligations, especially for services involving health, social care, or law enforcement.

Version History

The version history panel provides a history of the changes made to the document from the initial draft to the current version.

Version	Changes made	Date	Made by
0.1	Draft created	11 th September 2025	Clerk
1.0	Document approved by Councillors	17th September	Clerk