ST CUTHBERT (OUT) PARISH COUNCIL
c/o Mendip District Council, Cannard's Grave Road, Shepton Mallet, BA4 5BT
E-mail: parishclerk@stcuthbertout-pc.gov.uk
Tel: 07498 780143

DATA SECURITY BREACH REPORTING FORM

Introduction

A data security breach can happen for a number of reasons: Loss or theft of data or equipment on which data is Stored, Inappropriate access controls allowing unauthorised use, Equipment failure, Human error, Unforeseen circumstances such as a fire or flood, Hacking attack, 'Blagging' offences where information is obtained by deceiving the organisation who holds it.

Example: Reportable theft or loss of an unencrypted laptop computer or other unencrypted portable electronic/digital media holding names, addresses, dates of birth and National Insurance Numbers of individuals. A manual paper-based filing system (or unencrypted digital media) holding the personal data relating to named individuals and their financial records etc. More information can be found using this link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

Use this form to report such breaches.

Date and time of Notification of Breach	
Notification of Breach to whom: Name Contact Details	
Details of Breach	
Nature and content of Data Involved	

Number of individuals affected	
Name of person investigating breach: Name Job Title Contact details Email Phone number Address	
Information Commissioner informed: Time and method of contact Report a data breach to the ICO	
Police Informed if relevant: Time and method of contact Name of person contacted Contact details	
Individuals contacted: How many individuals contacted? Method of contact used to contact? Does the breach affect individuals in other EU member states? What are the potential consequences and adverse effects on those individuals? Confirm the details of the nature of the risk to the individuals	

affected and any measures they can take to safeguard against it. Relay to the individuals the likely cost to them of taking those measures.	
Staff briefed	
Assessment of ongoing risk	
Containment Actions: technical and organisational security measures you have applied (or were to be applied) to the affected personal data	
Recovery Plan	
Evaluation and response	