CALLINGTON TOWN COUNCIL

DATA SECURITY INCIDENT PROCEDURE

1. INTRODUCTION

1.1 We have a responsibility to ensure that personal information is kept and used securely. If anything goes wrong and, for example, data is lost, stolen, misused, sent to the wrong address or inappropriately accessed or released, we equally have a responsibility to put things right.

1.2 All suspected information security incidents must be reported to the Data Protection Officer (DPO). This enables the DPO to conduct a full investigation, and to identify areas of weakness and improvements that need to be made. It also enables the DPO to take a decision as to whether the incident should be reported to the Information Commissioner's Office as a data breach. The latter must be done within 72 hours of discovery, therefore all suspected incidents must be reported to the DPO as soon as they are discovered.

1.3 When sensitive information has been put at risk, but has not actually been lost, stolen, misused or inappropriately accessed or released, it may not be an incident requiring reporting to the Information Commissioner's Office however it is not good practice. For example, a member of staff taking sensitive information home without authority but returning it safely the next day would have put data at risk. The DPO will still put measures in place to prevent a reoccurrence.

1.4 All staff and councillors must be made aware of this procedure.

2. PROCEDURE

2.1 All identified incidents must be reported to the DPO as soon as they are detected. Even where there is some difference of opinion regarding breach, err on the side of caution and report it.

2.2 Upon detecting a breach, it is important to act quickly. In particular it is important to let the DPO know the following:

- The extent of the breach
- The amount of information involved
- The sensitivity of information involved

2.3 The DPO will investigate the incident and establish why it happened, whether or not it constitutes a breach and what remedial action is necessary.

2.4 The DPO will use their initial assessment to report the breach if it meets the necessary threshold for reporting to the Information

Commissioner's Office within 72 hours of the discovery of the breach. If this is done after 72 hours, the DPO will provide an explanation for this.

2.5 The DPO will prepare an incident report containing the following:

- A timeline of dates and times concerning the incident
- The potential for loss or damage to individuals, the parish council or any other body
- What measures need to be taken and how quickly to address:-

    i. Restoring any lost information to our custody or control

    ii. Whether to warn people about the loss, including who to warn and when. This may require a risk assessment.

    iii. Factors taken into account for deciding to report the loss to the Information Commissioner's Office.

    iv. Whether to report the loss to the Police.

2.6 The DPO will consider taking statements from those involved, especially where the quality of evidence may be lost through time or people may not be present for long.

2.7 The DPO will report any actions that need to be taken to prevent a reoccurance of the breach and the parish council will ensure that these are implemented.

2.8 The DPO will write to any data subject(s) affected, if necessary dependant on the outcome of a risk assessment, and deal with any subsequent complaint. A standard letter template for this is in Appendix 1.

2.9 The DPO will also correspond as applicable with any member of the public reporting a breach.

2.10 The DPO will deal with any correspondence from the Information Commissioner's Office, providing any further information requested and implementing any recommendations.