DYMOCK PARISH COUNCIL

DATA SECURITY INCIDENT PROCEDURE

Introduction

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

All suspected information security incidents must be reported. This enables a full investigation to be conducted, and for mitigating measures to be put in place. It also enables a decision to be made as to whether the incident should be reported to the Information Commissioner's Office as a serious data breach. The latter must be done within 72 hours of discovery, therefore all suspected incidents must be reported as soon as they are discovered. Reporting and investigating all data incidents enables areas of weakness to be identified and improvements to be made.

Not all data breaches will be sufficiently serious enough to meet the threshold for reporting to the ICO, however all data incidents and breaches must be dealt with.

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. This should still be logged as a potential data incident, allowing for investigation, improvement and measures to be put in place to prevent a reoccurrence or future data breach.

All staff, councillors, volunteers etc must be made aware of this procedure.

Procedure

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

Upon detecting a breach, it is important to act quickly. In particular it is important to report and identify the following:

- The extent of the suspected breach
- The amount of information involved
- The sensitivity of information involved
- A timeline of dates, times and events concerning the incident
- What personal data is involved
- The potential for loss or damage to individuals, the Parish Councils or others
- What measures need to be taken and how to quickly address –
  - Restoring any lost information to our custody or control
  - Whether to warn people about the loss, including who to warn and when.

- Whether to report the incident to the ICO
- Whether to report the incident to the Police

The incident will be further investigated by the Chair of the Parish Council to establish how and why it happened, whether or not it constitutes a breach and what remedial action is necessary.

This initial assessment will be used 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.

The Clerk 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.

An officer appointed by the Chair or the Clerk 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.

An officer appointed by the Chair or the Clerk will recommend any actions that need to be taken to prevent a reoccurance of the breach and the Parish Council will ensure that these are considered and where approved, implemented.

An officer appointed by the Chair or the Clerk 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.

An officer appointed by the Chair or the Clerk will also correspond as applicable with any member of the public reporting a breach.

An officer appointed by the Chair or the Clerk will deal with any correspondence from the Information Commissioner's Office, providing any further information requested and implementing any recommendations.

Golden rules for reporting and investigating data breaches

A serious breach must be reported by the Clerk to the ICO within 72 hours.

Observe the following "golden rules":

- Do not keep a breach to yourself, even if you feel there has been no harm arising. Next time – we may not be so lucky.

- Do not seek to apportion blame – the main object of this procedure is to close the breach and better ourselves as a result of it. Instances of wilful breach will be few and far between.
- This procedure is not confined to breaches involving personal data only. Any uncontrolled information loss is important.
- Be honest with the facts.
- Be thorough in investigating or assisting with any investigation.

Adopted

To be reviewed annually.

APPENDIX 1

Letter to notify that personal data has been breached

I write to you to bring to your attention a breach of the Data Protection Act that unfortunately involves your personal data.

As you would imagine we have taken this matter very seriously and *are investigating the matter / have concluded our investigation into it.*

The facts in this matter are *<give brief description of what has happened, eg a letter intended for you was sent to another individual because of an administrative error. The other individual immediately notified me on receipt and returned the letter.>*.

I am unable for reasons of confidentiality to go into details of my investigation, however I am able to tell you that you *<state what remedial action(s) have been carried out / what has been to prevent a reoccurrence, without breaching confidentiality>*

If you have any questions or concerns regarding this letter, please get in touch with me *or alternatively speak to your social worker who is aware of the situation*.

I would again like to apologise for the incident of which you were no doubt unaware.

Yours sincerely,

APPENDIX 2

Letter in response to notification by service user

Thank you for your *letter / telephone call* of <*date*> bringing the incident whereby <*state what has happened*> to our attention. We are obliged to you for acting in such a responsible way in contacting us.

As you would imagine we have taken this matter very seriously and I have concluded our investigation into it.

The facts in this matter are <*give brief description of what has happened, eg a letter intended for another individual was sent to you because of an administrative error*>.

I am unable for reasons of confidentiality to go into details of my investigation, however I am able to tell you that you <*state what remedial action(s) have been carried out / what has been to prevent a reoccurrence, without breaching confidentiality*>

I hope this letter has allayed your fears as to the integrity of your own information and documents and can I again thank you for bringing this case to our attention enabling us to take appropriate action.

Yours sincerely,