# STUDLAND PCC – DATA BREACH POLICY

## 1.0 Introduction

1.1 Studland PCC holds, process and share personal data that needs to be suitably protected.

1.2 Every care is taken to protect personal data from incidents (either accidental or deliberate) to avoid a data protection breach that could compromise security.

## 2.0 The Purpose

2.1 The Studland PCC is obliged under the Data Protection Act 1998 and updated General Data Protection Regulations May 2018 to have a framework designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility.

2.2 This Policy sets out the procedures to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents within Studland PCC.

## 3.0 The Scope

3.1 This Policy relates to all personal and sensitive data held by Studland PCC.

3.2 The objective of this Policy is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches.

## 4.0 Definition/Types of Breach

4.1 For the purpose of this Policy, data security breaches include both confirmed and suspected incidents.

4.2 An incident is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed and could cause material or emotional harm to the individual.

4.3 An incident includes but is not restricted to the following:

- Loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad/tablet device, 3rd party risk for information stored on a Cloud or paper record)
- Equipment theft or failure
- Unauthorised use of, access to or modification of data or information systems
- Attempts (failed or successful) to gain unauthorised access to information or IT system(s)
- Unauthorised disclosure of sensitive/confidential data
- Website defacement
- Hacking attack
- Unforeseen circumstances such as a fire or flood

- Human error
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it

**5.0 Reporting an incident**

5.1 Any individual who accesses, uses or manages information held by Studland PCC is responsible for reporting data breach and information security incidents immediately to the Data Protection Officer/Data Controller or as soon as is practicable.

***5.2*** The report will include full and accurate details of the incident, when the breach occurred (date and times), who is reporting it, if the data relates to people, the nature of the information, and how many individuals are involved. An Incident Report Form should be completed as part of the reporting process. ***See Appendix 1***

**6.0 Containment and Recovery**

6.1 The Data Protection Officer/Data Controller will determine if the breach is still occurring, if so, the appropriate steps will be taken immediately to minimise the effect of the breach.

6.2 An assessment to establish the severity of the breach will be undertaken and if anything can be done to recover any losses and limit the damage the breach could cause.

6.3 The Data Protection Officer/Data Controller will establish who may need to be notified as part of the initial containment.

**7.0 Investigation and Risk Assessment**

7.1 The Data Protection Officer/Data Controller will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.

7.2 The investigation will need to take into account the following:

- Type of data involved
- Its sensitivity
- The protections that are in place (e.g. encryptions)
- What's happened to the data, has it been lost or stolen
- Whether the data could be put to any illegal or inappropriate use
- Who the individuals are, number of individuals and the potential effects on those data subject(s)
- Whether there are wider consequences of the breach

**8.0 Notification**

8.1 The Data Protection Officer/Data Controller will determine who needs to be notified of the breach.

8.2 Every incident will be assessed on a case by case basis; however, the following will need to be considered:

- Whether there are any legal/contractual notification requirements.
- Whether notification would assist the individual affected – could they act on information to mitigate risks?
- Whether notification would help prevent the unauthorised or unlawful use of personal data?
- If a large number of people are affected, or there are very serious consequences, whether the Information Commissioner's Office (ICO) should be notified. (ico.org.uk or Telephone helpline 0303 123 1113)
- The dangers of over notifying. Not every incident warrants notification and over notification may cause disproportionate enquires and work.

8.3 Notifications to the individuals whose personal data has been affected by the incident will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate risks.

8.4 All Actions will be recorded by the Data Protection Officer/Data Controller.

**9.0 Evaluation and response**

9.1 Once the initial incident is contained, the Data Protection Officer/Data Controller will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, safeguarding, policies and procedures should be undertaken.

9.2 Existing controls will be reviewed to determine their accuracy and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

9.3 The review will consider:

- Where and how the personal data is held and where and how it is stored.
- Where the biggest risks lie, and will identify any further potential weak points within its existing measures.
- Whether methods of transmission are secure; sharing minimum amounts of data necessary.
- Identifying weak points within existing security measures.
- Awareness of all those who hold data within Studland PCC.

9.4 If deemed necessary a report recommending any changes to systems, safeguarding, policies and procedures will be considered by the PCC of Studland.

*APPENDIX 1*

**PCC OF STUDLAND - DATA BREACH REPORT FORM**

| | | |
|---|---|---|
| | **Report prepared by:**<br><br>**Date:** | |
| 1 | **Summary of the event and Circumstances** | *(When, what, who, summary of incident etc.)* |
| 2 | **Type and amount of personal data** | *(Title or name of documents. What personal Information it included – name, address DoB, bank account details, description of information about an individual)* |
| 3 | **Actions taken by the recipient when they inadvertently received the information** | |

| | | |
|---|---|---|
| 4 | **Actions taken to retrieve information and respond to the breach** | *(Has information been retrieved? When? Has loss been contained? e.g. all emails deleted)* |
| 5 | **Procedures/instructions in place to minimise risks to data security** | *(Communication, data storage, sharing and exchange)* |
| 6 | **Breach of procedure/policy** | *(Has there been a breach of policy? Has appropriate action been taken?)* |
| 7 | **Details of notification to affected data subject**<br><br>**Has a complaint been received from data subject** | *(Has the data subject been notified? If not, explain why not? What advice given to affected data subjects?)* |

| | | |
|---|---|---|
| 8 | **Procedure changes to reduce risks of future data loss** | |
| 9 | **Conclusion** | *(Serious/minor breach, likelihood of happening again. Report to ICO. Report to PCC)* |

**PCC of Studland**

**Charity Registration Number 1124710**