WHIMPLE PARISH COUNCIL
DATA BREACH POLICY & REPORT FORM

1. Introduction

1.1 Whimple Parish Council ("the Council") collects, holds, processes and shares personal information collected from a variety of different sources. Personal information is a valuable asset which can be seriously abused in the wrong hands, often causing great distress and inconvenience to the data subject.

1.2 Data breaches are increasingly common occurrences, whether through human error or malicious intent.

1.3 It is therefore necessary for the Council to have in place a robust policy and procedure for responding to any reported data breach, to ensure that it can protect as far as possible the security of any personal data that may come into its possession .

1.4 This Policy links to the Council's Data Protection Policy and the General Data Protection Regulations.

2. Purpose and Scope

2.1 The Council is obliged under the GDPR and related legislation to have in place a framework designed to protect the security of all personal data that comes into its possession. This includes clear lines of responsibility for the reporting and management of situations where there has been an apparent breach of data protection principles.

2.2 By adopting a systematic procedure to all reported data breaches the Council aims to ensure, inter alia, that:

- incidents are reported in a timely manner and can be properly investigated
- incidents are dealt with by appropriately authorised and skilled personnel
- there is appropriate level of involvement from the Parish Clerk as Proper Officer and designated Data Protection Officer and councillors
- incidents are recorded and documented
- lessons are learned from incidents and recommendations/procedures are adopted to prevent future re-occurrences
- evidence is gathered and decisions reached in such a way as to withstand external examination
- data subjects and external bodies are notified in a timely manner
- action is taken to minimise the impact of the breach

2.3 This policy sets out the procedure to be followed to ensure a consistent and effective approach for managing data breaches.

2.4 This policy applies to officers and councillors. This includes temporary, casual or agency staff as well as contractors, consultants, suppliers and data processors working on behalf of the Council. The policy needs to be read in conjunction with any HR policies and IT policies which may impact upon data security.

2.5 This policy applies to all personal and special categories of data held by the Council regardless of format.

3. Definitions and examples of breach

3.1 The Information Commissioner's website describes a breach as *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data."*

3.2 For the avoidance of doubt, this policy applies to both a *confirmed* breach and a *suspected* breach. Only a report and subsequent investigation will confirm whether there has been an actual breach and even in the event of the report being a false alarm, it may throw up issues of good practice to review.

3.3 Personal data breaches can include (this is not an exhaustive list):

- access by an unauthorised third party
- deliberate or accidental action (or inaction) by a controller or processor
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission
- loss of availability of personal data

4. Reporting an Incident

4.1 Any individual who uses or accesses the Council's information is responsible for its security. In the event of a confirmed or suspected data breach, the individual should immediately report the incident to the Parish Clerk.

4.2 If a breach is discovered outside normal working hours, it must be reported as soon as practicable. If this occurs over a bank holiday the Parish Clerk, who also acts as the Data Protection Officer, will be contacted via their mobile telephone number.

4.3 Any councillor or officer who believes or suspects that a data breach has occurred must complete a Data Breach Report Form (Appendix 1) and send it to the Parish Clerk by email (whimpleparishcouncil@gmail.com) within 4 hours of becoming aware of the existence of the breach. This is so even if all the facts are not yet available.

4.4 The Data Breach Report Form should be completed as fully as possible. As a minimum it should contain:

- the facts relating to the breach
- the effects of the breach
- remedial action taken

4.5 If further facts come to light after the submission of the Data Breach Report Form, these should be forwarded, without delay, to the Parish Clerk.

4.6 The Parish Clerk will investigate the breach. If the data breach has originated from the Parish Clerk, the Data Protection Officer from another Town or Parish Council will be approached and asked to investigate the matter.

4.7 The Parish Clerk will:

a) immediately upon being instructed:
- determine if the breach is still on-going and authorise the appropriate steps to minimise the effect of the breach

b) within 24 hours of being instructed:
- advise on the severity of the breach to councillors
- establish what can be done to recover any losses or minimise the damage the breach could cause
- advise whether any third parties need be notified – this is not limited to the data subject. It could include the police or data subject's bank.
- form a provisional view on whether the breach ought to be reported to the Information Commissioner's Office

c) within 48 hours of being instructed:
- produce a final breach report and recommendations which will, as a minimum, include:
  - A summary of the evidence
  - A summary of the legal position
    - A detailed assessment of the breach together with a recommendation as to whether the breach should be reported to the Information Commissioner
  - Advice on the impact and scale of the breach
    - A list of recommendations to prevent similar breaches in the future + a timetable for implementation
  - Details of all actions taken by the Council and the Parish Clerk to date

4.8 Employees should be aware that any breach of data protection legislation may result in the Council's disciplinary procedures being instigated. Employees, agency staff and casual workers may risk losing employment. Contractors and consultants may risk losing their contract with the Council.

5. Seriousness of the Breach

5.1 There is now a mandatory requirement to notify the Information Commissioner's Office of any notifiable breach with 72 hours of the Council becoming aware of the breach. This is not a lot of time, hence the rather short time scales imposed upon the Investigating Officer in section 4.

5.2 If breaches are reported to the Information Commissioner's Office then it is important that as much information as possible is made available to enable their office to fully investigate the breach and to recognise not only what has happened but also what we as a Council have done to minimise the effect of the breach and what steps have been taken to prevent a re-occurrence.

5.3 Every incident will be assessed on a case by case basis. To establish the severity of any breach, it is necessary to establish the likelihood and severity of the resulting high risk (arising from the breach) to people's rights and freedoms.

5.4 In short, if there is a risk then the breach must be reported. If a risk is unlikely, then it need not be reported although a record of the decision has to be kept.

5.5 By way of an example – the theft of a customer database will have to be reported because of the likelihood of identity fraud and the resulting distress that can cause. The loss of an internal directory of phone numbers need not.

5.6 Given the short time scale involved, it is appropriate that the decision whether to report a breach to the ICO shall be taken by the Council's Parish Clerk in consultation with the Chair & Vice Chair.

5.7 Any decision to report a breach to the Information Commissioner's Office shall be communicated by the Parish Clerk to councillors who shall be kept fully appraised as to the progress of the matter.

5.8 The Council shall keep secure records of:

- the Data Breach Report Form
- any advice or recommendations issued by the Investigating Officer either immediately or within 24 hours of being instructed
- a copy of the final Breach Report
- a copy of any decision to notify (or not) the Information Commissioner's Office of any breach
- any decisions in respect of third-party notifications

6. Notification

6.1 As noted in paragraph 4, the Parish Clerk will recommend whether anyone should be notified of the breach. There is an obvious reason for notification – so that the data subjects concerned can perhaps take immediate steps to limit the impact upon themselves and to also advise them that their data has been compromised.

6.2 There is a danger in "over-notification", so care will need to be exercised in deciding who to notify.

6.3 Individuals whose personal data has been affected by the breach and where it has been established likely to result in a high risk of adversely affecting that individual's rights and freedoms must be informed without undue delay. The notification will include a description of how and when the breach occurred, and the data involved. Advice must be offered about what they can do to protect themselves. The notification must also set out what has been done and provide a point of contact for the individual at the Council.

6.4 Consideration should also be given to notifying other third parties – eg, banks, insurers and the police. This may be appropriate if criminal activity is suspected.

7. Review

7.1 Following any breach, a review will be undertaken to see what lessons can and should be learned. This may result in changes to policy and practice.

8. Policy Review

8.1 This policy is a living document and will be reviewed and updated as necessary by the Parish Clerk. However, the Policy will be scrutinised annually to ensure its ongoing fitness for purpose.

APPENDIX 1
WHIMPLE PARISH COUNCIL – DATA PROTECTION BREACH NOTIFICATION FORM

- To be completed by the Parish Clerk as soon as practicable after the breach is notified

1. Summary of Incident	
Date and time of incident:	
Number of people whose data is affected:	
Nature of breach e.g. theft/disclosed in error/technical problems	
Description of how breach occurred:	

2. Reporting	
When was breach reported?	
How the Parish Clerk became aware of the breach:	
Have there been similar incidents in the past? If so, please provide details:	

3. Personal Data	
Full description of personal data involved (without identifiers):	
Number of individuals affected:	
Have all affected individuals been informed:	
If not, state why not:	
Is there any evidence to date that the personal data involved in this incident has been inappropriately processed or further disclosed? If so, please provide details:	

4. Data Retrieval	
What immediate remedial action was taken:	
Has the data been retrieved or deleted? If yes - date and time:	

5. Impact	
Describe the risk of harm to the individual as a result of this incident:	
Describe the risk of identity fraud as a result of this incident:	
Have you received a formal complaint from any individual affected by this breach? If so, provide details:	

6. Management	
Do you consider the individual(s) involved has breached information governance policies and procedures:	
If “yes”, why?	
Had the individual(s) completed data protection training:	
As a result of this incident, do you consider whether any other personal data held may be exposed to similar vulnerabilities? If so, what steps have been	

taken to address this:	
Has there been any media coverage of the incident? If so, please provide details	
What further action has been taken to minimise the possibility of a repeat of such an incident? Please provide copies of any internal correspondence regarding any changes in procedure:	

Form completed by…….

Position……..

Signed……

Email……...

Telephone Phone Number……..

Dated……...