Birchanger Parish Council
Personal Data Breach Policy

Document History

Version	Date	Remarks
1.0d1	27th September 2018	Candidate for adoption

Introduction

This policy describes the steps that are to be taken when it is known, or suspected, that the security of personal data controlled by the Council has been compromised.

What is a Personal Data Breach?

A personal data breach has taken place whenever the following happens to some personal data controlled by the Council.

- It has been lost, corrupted or destroyed
- It has been, or may have been, accessed by unauthorised persons
- It has been disclosed or altered without authorisation
- It has been used for purposes other than those for which it was provided

Examples of potential breaches include

- A laptop containing a copy of the electoral role is stolen
- A USB thumb drive containing personal data is lost
- A note book containing a written list of village residents is left in a public place

How are we notified of a Data Breach?

In many cases it will be the person handling the data who becomes aware of the breach, or potential breach. However, in some cases the notification will come from outside the council. The notification could be in writing or oral. In all cases the procedures below must be followed, but in the case of an oral notification the person making the notification should be asked to put it in writing. This policy should be put into action as soon as the notification is received even if a written version is not available.

Who Should be Notified?

All reports of breaches should be notified to the chairman within 24 hours. Upon receiving a notification the chairman should start the following process immediately. She/he would be expected to call upon the help of any councillor, the clerk to the council or other person or organisation who is be able to help, but the chairman must retain control of the situation.

Breach Handling Process

The breach handling process is as follows.

The chairman must immediately inform the council by email that a suspicion of a personal data breach has occurred, and they should be told the nature of the breach.

The first priority when handling a personal data breach is rectification and damage limitation. Immediate efforts must be made to limit any possible harm to those whose data has been compromised.

At an early stage an assessment must be made of:

- Whose personal data has been compromised?
- How damaging could this breach be to them?

The chairman must make this determination. She/he will probably do so by discussing the matter with councillors and the clerk, and may seek outside professional guidance if necessary from, e.g. the NALC. Based on all the facts a decision will be made as to whether the matter must be reported to the Information Commissioner's Office (ICO). This is a decision that may have serious consequences, so the chairman should read the latest ICO guidance, and should ensure that the council are fully involved.

If it is decided that the breach should be reported then the report must be made within 72 hours of the initial report of the breach. No allowances are made for holidays or weekends.

Informing the People Concerned

Any person whose personal data has been affected by a breach must be notified. The notification should tell them what has happened, how it could adversely affect them and what we are doing to remedy the situation. They should also be informed that they have the right to complain to the Information Commissioner's Office.

Record Keeping

A file of all decisions, with reasoning, should be kept of each breach or suspicion of a breach by the clerk.