STRADISHALL PARISH COUNCIL

PERSONAL DATA BREACH POLICY

Introduction

Stradishall Parish Council has a duty under the General Data Protection Regulation (GDPR) to ensure that the personal data it processes is kept safe and secure. This plan details how the Council will respond in the event of a personal data breach.

Purpose

This plan puts into place a procedure for dealing with any breaches of personal data which may occur, focussing on the steps to be taken once a breach has been discovered, and the processes that should be followed.

The Information Commissioner's Office (ICO) has the ability to impose significant fines on parish Council for serious contraventions of the GDPR.

This plan aims to provide a consistent approach and follows guidance provided by the ICO. However, dealing with incidents of breaches of data is complex; there are many potential variables and a balanced judgement needs to be taken on a case by case basis.

Aim

This plan sets out the Council's commitment to upholding the GDPR principles and managing the information we hold fairly and lawfully. It seeks to ensure that any personal or special category (sensitive) personal information the Council has in its possession is kept safe and secure and that processes are in place to minimise or mitigate the impact of a personal data breach.

Roles and responsibilities

This plan will be reviewed every year, or earlier, if necessary.

The Parish Clerk will be responsible for ensuring operational compliance with this plan and for seeking advice from others when appropriate.

Ensuring breaches do not happen

The effects of personal data losses are not only felt by the individuals concerned, but also affect the efficiency of the service and the reputation of the Parish Council as a whole.

It is important that all staff are aware of their responsibilities for handling personal information, keeping it secure and not disclosing it without proper cause.

All data controllers (the Council) have a responsibility to ensure appropriate and proportionate security of the personal data they hold. This is covered by the 6th principle of the GDPR as detailed below:

"[Personal data should be] processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')"

To prevent the Council from being in breach of the requirements of the GDPR the Clerk and all elected Members must be aware of their corporate and personal responsibilities set out under the provisions of the GDPR.

What is a personal data breach?

A personal data breach means 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.* This means that a breach is **more than just losing personal data.**

Such loss or release can occur in any of a number of ways:

- Loss or theft of equipment, which holds personal data e.g. laptops, tablets, CDs
- Loss or theft of hard copy documents
- Equipment failure
- Inappropriate access or unlawful access, allowing unauthorised use
- Human error
- Unforeseen incidents such as flood or fire
- Hacking attack
- Information obtained by surreptitious or deceptive means (blagging)
- Information being released inappropriately

Types of personal data breaches
Breaches can be categorised according to the following three information security principles.

- 'Confidentiality breach' - where there is an authorised or accidental disclosure of, or access to, personal data
- 'Availability breach' – where there is an accidental or unauthorised loss of access to, or destruction of, personal data
- 'Integrity breach' – where there is an unauthorised or accidental alteration of personal data

Dealing with a breach
As soon as a suspected or actual breach has been identified, the person who discovered it must report the incident immediately to the Parish Clerk, or, in their absence the Chairman. The Clerk will, at that point, become the 'breach owner'.

If a breach is suspected to have taken place the following information will be required in order to assess the seriousness of the potential breach:

- The type of data involved
- How sensitive the data is
- If the data has been lost or stolen, whether there are any protections in place e.g. encryption
- What has happened to the data?
- What could the data tell a third party about an individual
- The volume of data i.e. how many individuals' personal data are affected by the breach
- Who are the individuals whose data has been breached
- What harm can come to those individuals
- Are there wider consequences to consider e.g. loss of public confidence, negative publicity, financial implications

If after the initial assessment a breach has been clearly identified then a response should be co-ordinated by the Clerk in conjunction with the Chairman. Between them they will consider the action to be taken to:

- Protect the interests of the affected individuals
- Ensure the continuing delivery of the service
- Protect the interests of the Council
- Meet the requirements of the GDPR in terms of informing the Information Commissioner's Office

Breaches will require not just an initial response to investigate and contain the situation but also a recovery plan including, where necessary, damage limitation. Establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise

Notifying the Information Commissioner's Office (ICO)
The GDPR places a duty on all organisations to report certain types of data breach to the Information Commissioner's Office.

In the case of a personal data breach the Council shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the ICO, unless the personal data breach is **unlikely** to result in a risk to the rights and freedoms of natural persons. Where the notification to the ICO is not made within 72 hours, it shall be accompanied by reasons for the delay.

The GDPR states that a personal data breach should be reported to the ICO if the breach is likely to result in a risk to the rights and freedoms of the individuals concerned. By this it means discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. It also requires that this is done on a case by case basis. If there is not a risk to rights and freedoms, the ICO does not need to be notified.

After carrying out a full assessment of the risk, the decision as to whether or not to inform the ICO would normally rest with the Chairman of the Parish Council.

If the decision is to notify the ICO, the Parish Clerk will act as liaison with the ICO

The Chairman and any other relevant members will need to consider whether any officer concerned with the breach will be subject to disciplinary procedures.

The notification referred to above shall at least:

- Describe the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned

- Communicate the name and contact details of the Clerk or other contact point where more information can be obtained
- Describe the likely consequences of the personal data breach
- Describe the measures taken or proposed to be taken by the Council to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects

Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

The Council shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the ICO to verify compliance with the GDPR.

Failing to notify a breach when required to do so can result in a significant fine up to 10 million Euros; this is at the discretion of the ICO.

Communication of a personal data breach to the data subject

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Council shall communicate the breach to the data subject without delay. This risk exists when the breach may lead to physical, material or non-material damage for the individuals whose data have been breached. Examples of such damage are:

- Discrimination
- Identity theft or fraud
- Financial loss
- Damage to reputation

When the breach involves personal data that reveals racial or ethnic origin, political opinion, religion or philosophical beliefs, or trade union membership, or includes genetic data, data concerning health or data concerning sex life, or criminal convictions and offences or related security measures, such damage should be considered likely to occur.

The communication to the data subject shall describe in clear and plain language the nature of the breach and contain at least the information and the recommendations provided.

The communication to the data subject shall not be required if any of the following conditions are met:

- The Council has implemented appropriate technical and organisational protection measures, and that those measures were applied to the personal data affected by the breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption
- The Councils have taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise
- It would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

The Parish Clerk should consider consulting the ICO to seek advice about informing data subjects about a breach and on the appropriate messages to be sent to, and the most appropriate way to contact, individuals.

Consideration also needs to be given to any prospective equality issues that may arise from a breach e.g. the vulnerability of an individual affected by the breach.

Post breach evaluation

Once the immediate breach response actions have been completed it is important not only to investigate the causes of the breach, but to also evaluate the effectiveness of the response. Carrying on 'business as usual' may not be acceptable if systems, policies or allocation of responsibilities was found to be at fault. Improvements should be instigated as soon as possible and should be communicated to staff and recorded so the Council can be seen to have reacted in a responsible manner.

Those investigations into the cause of the loss of data should consider any staff capability or training issues that may be indicated and where appropriate, action may be considered under the Council's disciplinary procedure.

If the breach was caused, even in part, by systemic and ongoing problems, then action will need to be taken and procedures in place to prevent any recurrence in the future.