St Mawgan-in-Pydar Parish Council

Data Breach Policy and Procedure

St Mawgan-in-Pydar Parish Council is a Data Controller. The Parish Council is required to keep the personal data it holds secure, to identify when a breach has occurred and to know how to deal with a breach should one occur. All matters relating to data protection, including the handling of data breaches are delegated to the Clerk.

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. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Personal data breaches can include: • 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; and • loss of availability of personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

What to do when a breach occurs

The Clerk must be notified as soon as an employee or councillor becomes aware that it has occurred. This includes evenings, weekends, and holidays. The Clerk will obtain as much information as possible from the person reporting the breach. The Clerk will establish the likelihood and severity of the risk to people's rights and freedoms, referring to the guidance published by the Information Commissioner's Office. If it is likely that there will be risk, the Clerk will notify the Information Commissioner's Office via their website without undue delay and certainly within 72 hours of the time that the employee or councillor became aware that the breach occurred. If the Clerk concludes that there is unlikely to be a risk to people's rights and freedoms, then the breach will not be reported. The Clerk will make a clear record of the reasons for not reporting the breach. The Clerk will ensure that any and all steps are immediately taken to contain the breach and minimise the potential risk of harm to the people whose data has been breached. If the Clerk concludes that the breach is likely to result in a high risk to the rights and freedoms of individuals, the Clerk will consider whether the individuals affected should be informed directly, applying the assessment guidance published by the Information Commissioner's Office. Where necessary the Clerk will ensure that these individuals are informed directly and without undue delay to enable them to take steps to protect themselves from the potential effects of the breach. The Clerk will also consider whether it would be appropriate to notify third parties such as the police, insurers, professional bodies, or bank or credit card companies who can help reduce the risk of financial loss to individuals. When assessing how to deal with a breach the Clerk will ensure that the decision-making process is fully documented in accordance with the principle of accountability in data processing. The Clerk will

then carry out an investigation to determine how the breach occurred, whether any Council policies were breached and by whom, and what measures can be put in place to reduce the risk of a similar breach occurring in the future. If the breach is deemed to be due to any action or inaction by an employee or councillor, then there will be an assessment of whether it will be appropriate to invoke the Parish Council's Disciplinary Policy (for staff) or the Code of Conduct Policy (for councillors).

The role of external Data Processors

The Parish Council uses the following external organisations to store personal data: • Moneysoft to store the Parish Council's payroll data.

If an external processor suffers a breach, it is required to inform the Parish Council without undue delay as soon as it becomes aware. This requirement enables the Parish Council to take steps to address the breach and meet its reporting obligations under the GDPR.

Record Keeping

A record of all breaches will be maintained. The record will include the facts relating to the breach, its effects, the reasons why the breach was/was not reported to the Information Commissioner's Office and/or the individuals affected, and the remedial action taken.

Approved: 11 September

Minute Reference: 221/19 (j)

Reviewed annually or as a result of Information Commissioner's Office guidance