DATA BREACHES Policy

Blewbury Parish Council

Personal Data Breaches

- The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. We must do this within 72 hours of becoming aware of the breach, where feasible.
- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we must also inform those individuals without undue delay.
- We should ensure we have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not we need to notify the relevant supervisory authority and the affected individuals.
- We must also keep a record of any personal data breaches, regardless of whether we are required to notify

What is a personal data breach?

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 if you suspect a data breach has occurred

If you suspect a data breach has occurred contact the DPO (Data Protection Officer) or in the interim the Data Processor (Parish Clerk)

When a personal data breach has occurred, we need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then we must notify the ICO; if it's unlikely then we don't have to report it. However, if we decide we don't need to report the breach, we need to be able to justify this decision, so we should document it.