Data Breach Policy

A personal data breach is one that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. 1. Notifying the Information Commissioners Office (ICO) Currently, data breaches do not have to be routinely notified to the ICO or others although the ICO recommends that it is good practice so to do. However, guidance states that organisations should notify the Information Commissioners Office of a breach where it is likely to result in a risk to the rights and freedoms of individuals or if it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. Data Breaches will be recorded using the ICO's online system: https://ico.org.uk/for-organisations/report-a-breach/ and the following information should be provided: • The potential scope and cause of the breach • Mitigation actions the council plans to take • Details of how the council plans to address the problem. 2. Notifying the Individual concerned If a breach is likely to result in a high risk to the rights and freedoms of individuals (such as through identity theft) the council will notify those concerned. 3. Timescales Under the GDPR, we are required to report a personal data breach, which meets the reporting criteria, within 72 hours to the Information Commissioner. In line with the accountability requirements, all data breaches must be recorded by the parish council along with details of actions taken. This record will help to identify system failures and should be used to improve the security of personal data. 4. Notifying the council If anyone (including a third party such as a payroll provider) suspects that a data breach has occurred details of the alleged breach should be submitted immediately in writing to: Clerk: John Fleming Fell View Blencarn Penrith Cumbria CA10 1TX Tel: 07768 468 634 E-mail: langwathbypc@hotmail