FINMERE PARISH COUNCIL DATA BREACH POLICY

Definition – a breach of security leading to 'accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.'

Councillors, staff, contractors and the council's data processors should be briefed in advance on how to avoid a personal data breach and on what to do in the event that a breach occurs.

Examples of personal data breaches and steps to avoid them include:

- Emails and attachments being sent to the wrong person, or several people. – Slow down, check thoroughly before clicking 'send.'
- The wrong people being copied in to emails and attachments – Use BCC (Blind Carbon Copy) where necessary.
- Lost memory sticks which contain unencrypted personal data – the council should put protocols in place for memory stick usage – any storage device must be encrypted and kept secure.
- Malware (IT) attack – ensure up to date anti-virus software is in place.
- Equipment theft – check security provisions.
- Loss of personal data which is unencrypted – maintain encryption protocols.

All councillors, staff, contractors and the council's data processors should be aware of the risks of a breach and alert to the occurrence of any breach, with regular checks and with regard to best practice.

Any breach should be reported to the Parish Clerk or, in their absence, the Chairman of the PC.

A record shall be kept of any breach.

The DPO, if one has been appointed, must be informed.

A determination must be made by the Clerk and the Chairman, or the Vice Chairman if either is absent, in consultation with the DPO if one has been appointed, as to whether the breach meets the criteria for reporting to the ICO or the person whose data is concerned in the breach. If so the report must be made within 72 hours. (Unauthorised access to data that could be used to steal someone's identity such as their banking data must be reported).