Data Protection Breach

St. Michael and All Angels' Church takes its responsibility under the data protection legislation (GDPR) legislation seriously and is committed to ensuring that all personal data which is held is done so in a secure manner and that only authorised individuals have access to the data.

A personal data breach means 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.

Anyone can report a breach to the Rector and Churchwardens.

Breach Process

The following process will be followed:

1) A breach is identified
2) Rector and Churchwardens are informed
3) Record the breach on the log which will ensure that appropriate corrective actions are implemented.
4) Within 7 days, Rector and Churchwardens assess the severity of the breach and identify the root cause of breach. The items assessed be the likelihood and severity of the resulting risk to people's rights and freedom (section 85 of GDPR). This includes
    a. Result in physical, material or non-material damage include but not limited to,
        i. Loss of control over their personal data
        ii. Limitation of their rights
        iii. Discrimination,
        iv. identity theft or fraud
        v. Financial loss
        vi. Damage to reputation
5) Identify the people affected by the breach.
6) Review the policies, procedures and training.
7) The Churchwardens/Rector will notify the Diocesan Secretary, the Diocesan registrar and if advised the Information Commissioner within 72 hours (GDPR mandatory timeline)
8) If applicable, inform the individuals affected about the breach.

Failure to report a breach to the ICO (if required) can result in a significant fine up to 2% of our turnover.

Sample Data Breach Log

Date	Details of Breach	Person Reporting	Severity	Corrective Actions

Approved by PCC 8-May-2019