BRADFIELD ST GEORGE PARISH COUNCIL

Personal data breaches policy

APPROVED 10th MAY 2023

Next review date May 2027

Bradfield St George Parish Council is a data controller for the purpose of the General Data Protection Regulations (GDPR). The Clerk to the Parish Council is the data manager for these purposes. Further information regarding personal data is set out in the Bradfield St George PC privacy notice on the website https://bradfieldstgeorge.suffolk.cloud. From 25 May 2018 data controllers have new obligations to (i) keep an internal record of all personal data breaches, (ii) report them within 72 hours to the ICO in certain circumstances and (iii) notify an individual affected by a personal data breach in certain circumstances.

A personal data breach is defined for GDPR as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed. Examples of a personal data breach include but are not limited to sending personal data to the incorrect recipient, computing devices being stolen or hacked or lost, alteration of personal data without permission etc.

In the event of a data breach, the data controller will undertake an investigation within one month of the report of a breach. Procedures are in place to detect, report and investigate a personal data breach, following the advice set out in *NALC note L02-18 – Reporting personal data breaches*. The ICO will be advised of a breach (within 3 days) where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality, or any other significant economic or social disadvantage. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the data controller will also have to notify those concerned directly.

Employees, staff and volunteers of the Council are aware of this policy and know that (i) any personal data breach must be reported to the data manager as soon as it is noticed; (ii) full cooperation is required to address a personal data breach as soon as possible in order to mitigate any negative consequences and (iii) reasonable steps to minimise the risk of any such personal data breach are required and in this regard, it is unacceptable for non-authorised users to be able to access staff/volunteers IT using employees/volunteers' log-in passwords or to use equipment while logged on. It is unacceptable for employees, volunteers and members to use IT in any way that may foreseeably lead to a personal data breach..