Data Breach Policy

1. Data Breach Response

1.1 A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or processed.

1.2 The following are examples of data breaches:

- access by an unauthorized third party;
- deliberate or accidental action (or inaction) by a data controller or data processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission;
- loss of availability of personal data.

1.3 This Council understands that planning for a breach is essential to ensure that it has a process in place to deal with a breach at short notice should it occur. Kingsbury Parish Council takes the security of personal data seriously; computers are password protected, the hard drives encrypted and hard copy files are stored securely.

2. **Consequences of a Personal Data Breach**

2.1 A breach of personal data may result in a loss of control of personal data, discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of personal data, damage to property or social disadvantage. Accordingly, a breach, depending on the circumstances of the breach, can have a wide range of effects on individuals.

2.2 The Breach Response Plan below sets out the key issues which the council has considered in preparing for a data breach.

2.2.1 The Data Protection Officer and Chair should be notified immediately of a suspected breach without delay. It is then the Data Protection Officer responsibility to inform the ICO; it is not the data processors responsibility to notify the ICO.

2.2.2 The Data Protection Officer and Chairman will take responsibility with delegated authority to manage the breach. An extraordinary meeting of the Council may be called if required.

2.2.3 In the event of a breach an investigation will be carried out. This investigation will be carried out by the Data Protection Officer who will decide whether the breach is required to be notified to the Information Commissioner. A decision will also be made over whether the breach is such that the individual(s) must also be notified.

2.2.4 We will undertake to notify the Information Commissioner of a breach which is likely to pose a risk to people's rights and freedoms. A risk to people's freedoms can include physical, material or non-material damage such as discrimination, identity theft or fraud, financial loss and damage to reputation. Notification to the Information Commissioner will be done without undue delay and at least within 72 hours of discovery.

If we are unable to report in full within this timescale, we will make an initial report to the Information Commissioner, and then provide a full report in more than one installment if required. The following information will be provided when a breach is notified:

- A description of the nature of the personal data breach including where possible, the categories and approximate numbers of individuals and person date records concerned
- The Name and contact details of the Data Protection Officer (see below)
- A description of the likely consequences of the personal data breach
- A description of the measures taken, or proposed to be taken, to deal with the breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

2.3 The Clerk and Data Protection Officer will consult other data controllers or contractors as a matter of urgency for any external assistance as necessary and this is covered in the Council's Privacy Policy and Subject Access Policy.

2.4 The Clerk along with the Data Protection Officer may, depending upon the nature of the breach, need to contact others to identify any actual breach and activate a breach response team if the extent of the breach requires.

2.5 The Council will review its response plan each year, testing the process with others if required.

2.6 The Clerk along with the Data Protection Officer will record all personal data breaches regardless of whether they are notifiable or not, as part of its general accountability requirement under GDPR. The Data Protection Officer will record the facts relating to the breach, its effects and remedial action taken.

3. Legal Issues

3.1 The Council will maintain legal privilege and confidentiality where required.

3.2 Should a pause of document destruction processes be required, the Data Protection Officer will instruct as necessary.

3.3 The Date Protection Officer along with the Clerk along with the will lead on gathering appropriate evidence and information about the breach.

3.4 The Council, if required will contact and/or legal advisers at North Warwickshire Borough Council to manage the investigation and give legal advice.

3.5 The Data Protection Officer along with the Clerk will ensure that steps to manage the investigation are recorded.

3.6 Contractual rights and obligations with third parties are set out in the Council's Privacy Policy.

3.7 The Council may need to notify third parties as set out in the Council's Data Management Policy and Audit Log.

3.8 The Council sets out its contractual rights within its policies and contracts with others.

3.9 The Council will contact the Information Commissioners Office ("ICO") and its local law enforcement officer where necessary.

3.10 The Council may take advice from its legal advisers on the legal options available to gather evidence from third parties.

3.11 The Data Protection Office along with the Clerk will consult with its legal advisers and/or insurers on potential

liabilities to third parties.

4. Information Technology (IT)

4.1 The Data Protection Officer along with the Clerk will consult with its IT supplier where required in managing potential risk and responding to a data breach.

4.2 The Council's asset register will identify devices where a potential breach may occur. (c) The flow of data is set out in the Council's Communication policy

4.3 The Data Protection Officer along with the Clerk will consult with its IT supplier to quickly secure and isolate potentially compromised devices and data, without destroying evidence should this be necessary.

4.4 The Data Protection Officer along with the Clerk will ensure the quick physical security of premises should this be necessary.

5. Cyber Breach Insurance

5.1 The Council takes advice from its insurers on cyber breach insurance and actions onnotifying and obtaining consents should a breach occur.

5.2 The Clerk and Date Protection Officer holds emergency contact details.

6. Data

6.1 Data held by the Council is set out in this Data Protection Policy and Data Inventory, which includes its classification, destruction time and risk assessments, which includes protections for any sensitive data.

6.2 The Date Protection Officer along with the Clerk liaises with its IT supplier. The council laptop has an encrypted hard drive and advice has been taken about secure passwords.

6.3 The Date Protection Officer along with the Clerk will ensure that data is held no longer than required according to the Document Retention policy.

7. Data subjects

7.1 The Council has in place Subject Access Request and Privacy Policies with appropriate notices which are published on its websites: These include notifying data subjects and contractual and legal rights of data subjects.

7.2 The Council will provide appropriately worded notifications to data subjects.

7.3 The Council has in place its policies and notices in compliance with GDPR, recognizing the potential harm to data subjects should loss of data held by the Council occur.

7.4 The Council is committed to arranging appropriate training for councilors and staff with includes action in the event of a breach.

8. Public Relations

8.1 The Council will consult its legal advisers in dealing with data breaches particularly with pro-active and re-

active press statements.

8.2 The Council will put in place arrangements to monitor media reaction as required after any breach

9. Contacts

9.1 Please contact us if you have any questions about this Privacy Policy or the personal data we hold about you or to exercise all relevant rights, queries or complaints at:

The Data Controller, Parish Council Clerk email: kingsburypc@outlook.com
Data Protection Officer, Cllr Owen Phillips email: owenphillips@northwarks.gov.uk

10. Reviews

This policy will be reviewed frequently, and updated as required.

Adopted at the Parish Council Meeting on 18th September 2024 (Minute 388)
Review due September 2025

Revision Control

Revision	Details of Change
Sep 24	New