# Data Breach Response Policy

Adopted by the Council on…11 June 2018 Next Review Date……June 2019…

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

The following are examples of data breaches:

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

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.

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

(a) The Clerk should be notified immediately of a suspected breach and in the absence of the clerk, the Data Protection Officer and Chairman should be notified.

(b) The Clerk in consultation with 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.

(c) 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 make a decision over 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.

(d) 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 instalment if so 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.

(e) The Clerk 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.

(f) The Clerk 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.

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

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

**2. Legal issues**

(a) The Council will maintain legal privilege and confidentiality where required.

(b) Should a pause of document destruction processes be required, the Clerk will instruct as necessary.

(c) The Clerk will lead on gathering appropriate evidence and information about the breach.

(d) The Council if required will contact the Data Protection Officer and/or legal advisers at Shropshire Council to manage the investigation and give legal advice.

(e) The Clerk will ensure that steps to manage the investigation are recorded.

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

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

(h) The Council sets out its contractual rights within its policies and contracts with others.

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

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

(k) The Clerk will consult with its legal advisers and/or insurers on potential liabilities to third parties.

**3. IT**

(a) The Clerk will consult with its IT supplier where required in managing potential risk and responding to a data breach.

(b) 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

(d) 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.

(e) The Clerk will ensure the quick physical security of premises should this be necessary.

**4. Cyber breach insurance**

(a) The Council takes advice from its insurers on cyber breach insurance and actions on notifying and obtaining consents should a breach occur.

(b) The Clerk holds emergency contact details.

**5. Data**

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

(b) The Clerk liaises with its IT supplier. The council laptop has an encrypted hard drive and advice has been taken about secure passwords

(c) The Clerk will ensure that data is held no longer than required according to the Document Retention policy.

**6. Data subjects**

(a) 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.

(b) The Council will provide appropriately worded notifications to data subjects.

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

(d) The Council is committed to arranging appropriate training for councillors and staff with includes action in the event of a breach.

**7. Public Relations**

(a) The Council will consult its legal advisers in dealing with data breaches particularly with pro-active and re-active press statements.

(b) The Council will put in place arrangements to monitor media reaction as required after any breach.

**Changes to this policy**

We keep this Security Incident Policy under regular review and we will publish any updates on www.pontesburyparishcouncil.org.uk This Policy was last updated in June 2018.

Contact Details

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, 8 Holbache Rd, Oswestry, SY11 1RP Tel: 01691 661157

Email: clerk@pontesburypc.org.uk

Data Protection Office: JDH Business Services Ltd. Carreg Llwyd, Cefn Bychan Road, Pantmwyn, Flintshire. CH7 5EW