WEXHAM COURT PARISH COUNCIL
DATA BREACH PROCEDURE

1. Scope
a) This procedure applies in the event of a personal data breach.

b) The General Data Protection Regulations (GPDR) draws a distinction between a '*data controller*' and a '*data processor'* in order to recognise that not all organisations involved in the processing of personal data have the same degree of responsibility. Therefore, each organisation should establish whether it is a data controller or a data processor for the same data processing activity.

2. Responsibility
a) All users, whether employees/staff or temporary employees/staff and third-party users and Councillors of Wexham Court Parish Council are required to be aware of, and to follow this procedure in the event of a personal data breach.

3. Procedure – Breach Notification Data Processor to Data Controller
a) Wexham Court Parish Council will report any personal data breach to the data controller (Clerk) without undue delay.

4. Procedure – Breach Notification Data Controller to Supervisory Authority
a) In the event of a personal data breach, the Clerk (Data Controller) shall notify the supervisory authority (Information Commissioner's Officer) without undue delay of a personal data breach.

b) The Clerk assesses whether the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach.

c) If a risk to the aforementioned is likely, the Clerk shall report any personal data breach to the ICO without undue delay and where feasible, within no more than 72 hours. Where a data breach notification to the ICO is not made within 72 hours, it shall be accompanied by the reasons for the delay.

d) The data controller (Clerk) shall provide the following information to the Parish Council:

- A description of the breach
- The categories of personal data affected
- Approximate numbers of data subjects affected
- Approximate number of personal data records affected
- Likely consequences of the breach
- Any measures that have been or will be taken to address the breach, including mitigation

- The information relating to the data breach, which may be provided in phases
- The date and time the Clerk advised the ICO
- The notification is made by (email, phone)
- Confirmation of receipt of this information is made by email.

5. Procedure - Breach Notification Data Controller to Data Subject

a) Where the personal data breach is likely to result in high risk to the rights and freedoms of the data subject, Wexham Court Parish Council will notify the affected data subjects without undue delay.

b) The notification to the data subject shall describe in clear and plain language the nature of the breach, including the information specified in 4 (d) above.

c) Appropriate measures shall be taken to render the personal data unusable to any person who is not authorised to access it such as encryption.

d) The controller shall take subsequent measures to ensure that the rights and freedoms of the data subjects are no longer likely to be compromised.

e) If it would be a disproportionate amount of effort to carry out the above, there shall be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

f) The ICO may where it considers the likelihood of a personal data breach to result in high risk, require the data controller to communicate the personal data breach to the subject.

Data Protection Terminology

Data subject - means the person whose personal data is being processed.
That may be an employee, prospective employee, associate or prospective associate of London Colney Parish Council or someone transacting with it in some way, or an employee, Member or volunteer with one of our clients, or persons transacting or contracting with one of our clients when we process data for them.

Personal data - means any information relating to a natural person or data subject that can be used directly or indirectly to identify the person. It can be anything from a name, a photo, and an address, date of birth, an email address, bank details, and posts on social networking sites or a computer IP address.

Sensitive personal data - includes information about racial or ethnic origin, political opinions, and religious or other beliefs, trade union membership, medical information, sexual orientation, genetic and biometric data or information related to offences or alleged offences where it is used to uniquely identify an individual.

Data controller - means a person who (either alone or jointly or in common with other persons) (e.g. Council, employer, councillor) determines the purposes for which and the way any personal data is to be processed.

Data processor - in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Processing information or data - means obtaining, recording, or holding the information or data or carrying out any operation or set of operations on the information or data, including:

- organising, adapting, or altering it
- retrieving, consulting, or using the information or data
- disclosing the information or data by transmission, dissemination or otherwise making it available
- aligning, combining, blocking, erasing, or destroying the information or data. regardless of the technology used.

Adopted: March 2024