Wheatley Parish Council
Personal Data Breach Policy

Adopted 4th June 2018. Reviewed June 2021

Purpose of this policy
As part of the General Data Protection Regulation (UK-GDPR) the council is required to have procedures in place to ensure security of all its personal data and lines of responsibilities.

This policy should ensure that the council meets the requirements of legislation and to minimise risks associated with breaches.

Scope
This policy covers all types of personal data and includes hard copies and electronic data.

Personal data is information that can identify an individual (contact details, date of birth, bank details or information on their health, family or education)

It applies to all officers, councillors, consultants and contractors.

The council regularly reviews the data it stores.

Data breaches may be classified as confirmed or suspected incidents, this could include (but is not restricted to;

- loss or theft of sensitive or confidential data/equipment on which data is stored – USB stick, laptop, hard drive, tablet or paper copy
- unauthorised use or access to files or systems
- attempts to gain unauthorised access to files or systems
- altering personal data without permission
- human error (e.g., sending personal data to incorrect recipient)
- system failure

Reporting incidents
Anyone who becomes aware of breach should report this to the Clerk and Chairman immediately.
If this is outside of normal office hours, it must be reported as soon as possible.
Details of the incident should be reported using the Data Breach Report Form. (Appendix 1)

Any breach that is likely to result in a “risk to the rights and freedoms” must be reported to the ICO “without undue delay” and where practicable within 72 hours of being aware of it.
If the report it made outside of the 72 hours the report should include reasons for the delay.

The Clerk/chair should first determine whether the breach is still occurring. If so, appropriate steps should be taken to stop or minimise the breach.

An assessment should be undertaken by the Clerk/Chairman to establish who should undertake investigations into the breach, whether information can be recovered or reclaimed, whether the police should be informed, what internal or external advice or support should be sought.

Further investigations should be undertaken ideally within 24 hours and will assess the type of data involved, its sensitivity, protections currently in place, has the data been used illegally or inappropriately, who has been affected and what the consequences of the breach may be.

Notifications
If the breach is likely to have resulted in a “risk to the rights and freedoms” it must be reported to the ICO “without undue delay” and where practicable within 72 hours of being aware of it.
If the report it made outside of the 72 hours the report should include reasons for the delay.

Similarly, any individuals who may have been affected by the breach should be contacted without delay, with details on the data involved and how the breach has occurred. Clear guidance and advice should be given to reduce further risks to the individual.

The involvement of third parties (police, insurers, banking, and credit companies) will need to be considered based on the data involved and the nature of the breach.

Any breach will be reported to Full Council at the next available meeting.

Record Keeping
Records of any breaches, investigations and contact with individuals or third parties should be kept, regardless of whether the ICO is involved. Records will be stored in line with the council’s Retention and Disposal Policy

Evaluation and Resolution
A full review and report of the incident will be undertaken by officers/councillors covering the causes, responses, policies, procedures and security measures and controls.

The report will be presented to Full Council at the next available meeting.

Documentation Review
This and all UK-GDPR related documentation will be updated as and when changes in legislation occur. It will be reviewed annually in line with other policies.

References
NALC LO2-18 Reporting Personal Data Breaches