North Leverton with Habblesthorpe Parish Council

Data Breach Policy

Document Control	
Date	September 2021
Details	Next Review September 2022
Date	May 2022
Details	Previous Clerk details removed. Document Control set up. Next review due September 2023

GDPR defines a personal data breach as "a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed". Examples include:

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction) by a controller or 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

North Leverton with Habblesthorpe Parish Council takes the security of personal data seriously, computers shall be password protected and hard copy files shall be kept in locked cabinets or desk drawers.

Consequences of a personal data breach

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. Therefore a breach, depending on the circumstances of the breach, can have a range of effects on individuals.

North Leverton with Habblesthorpe Parish Council's duty to report a breach

Any data breach that is likely to result in a risk to the rights and freedoms of an individual shall be immediately reported to the Parish Council's Data Protection Officer (DPO) who shall report the breach to the individual concerned, and, to the Information Commissioner's Office (ICO). The DPO's reporting of the breach shall be undertaken without undue delay and, where feasible, not later than 72 hours after having become aware of the breach.

If the ICO is not informed within 72 hours, North Leverton with Habblesthorpe Parish Council's DPO must give reasons for the delay when they report the breach.

When notifying the ICO of a breach the PC's DPO shall:

1. Describe the nature of the breach including the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned
2. Communicate the name and contact details of the DPO
3. Describe the likely consequences of the breach
4. Describe the measures taken or proposed to be taken to address the personal data breach including, measures to mitigate any possible adverse effects.

When notifying the individual affected by the breach the PC's DPO shall provide the individual with the information stated in (2)-(4) above.

The PC's DPO need not communicate with an individual if the following applies;

- The PC has implemented appropriate technical and organisational measures (i.e encryption) so those measures have rendered the personal data unintelligible to any person not authorised to access it;
- The PC has taken subsequent measures to ensure that the high risk to rights and freedoms of individuals is no longer likely to materialise;
- The PC would be involved in disproportionate effort

The ICO shall still be informed even if the above measures are in place.

Records of data breaches

All data breaches shall be recorded on the record sheet provided whether or not they are reported to individuals. This record will help to identify system failures and should be used as a way to improve the security of personal data.

To report a data breach, use the ICO online system;

https://ico.org.uk/for-organisations/report-a-breach/

North Leverton with Habblesthorpe Parish Council – Record of Data Breaches				
Date of breach	Type of breach	Number of individuals affected	Date reported to ICO/individual	Actions to prevent breach recurring