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

Nettleham Parish Council takes the security of personal data seriously, computers are password protected and hard copy files are kept in locked cabinets.

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.

Examples of a Data Breach

- Emails sent to the wrong resident
- Electoral register left on display
- Personnel files lost
- Allotment waiting list emailed incorrectly
- Laptop stolen
- Councillor loses USB stick
- Cemetery records emailed incorrectly.

Immediate Response Procedure

If any member of staff or councillor discover a suspected breach the must immediately

- Contain the breach where possible
- Inform the Clerk to the Council immediately
- Preserve any evidence
- Record what has happened
- Do not attempt to conceal the breach
- Do not delete any emails or files
- Establish what information has been lost, is it personal data, how many people have been affected and what harm could result ?

Containment Measures of a Breach or Suspected Breach

Once a breach has been or suspected to have occurred you may contain such a breach by:-

Recalling an email

Disable user account(s)

Change passwords

Recover documents

Contact recipients

Investigation

Following a breach there should be a thorough investigation to establish:-

- Why and how did it happen ?
- Was procedure followed
- Is there a training need ?
- Is any disciplinary action necessary ?
- Does policy need updating ?

Nettleham Parish Council's duty to report a breach

If the data breach is likely to result in a risk to the rights and freedoms of the individual, the breach must be reported to the individual and ICO without undue delay and, where feasible, not later than 72 hours after having become aware of the breach. The Data Protection Officer must be informed immediately so they are able to report the breach to the ICO in the 72-hour timeframe.

If the ICO is not informed within 72 hours, Nettleham Parish Council via the DPO must give reasons for the delay when they report the breach.

When notifying the ICO of a breach, Nettleham Parish Council must:

i. 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;
ii. Communicate the name and contact details of the DPO;
iii. Describe the likely consequences of the breach;
iv. Describe the measures taken or proposed to be taken to address the personal data breach including, measures to mitigate its possible adverse affects.

When notifying the individual affected by the breach, Nettleham Parish Council must provide the individual with (ii)-(iv) above.

Nettleham Parish Council would not need to communicate with an individual if the following applies:

- It 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;
- It has taken subsequent measures to ensure that the high risk to rights and freedoms of individuals is no longer likely to materialise, or
- It would involve a disproportionate effort

However, the ICO must still be informed even if the above measures are in place.

Data processors duty to inform Nettleham Parish Council

If a data processor (i.e. payroll provider) becomes aware of a personal data breach, it must notify Nettleham Parish Council without undue delay. It is then Nettleham Parish Council's responsibility to inform the ICO, it is not the data processors responsibility to notify the ICO.

Records of data breaches

All data breaches must be recorded 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.

Record of Data Breaches

Date of breach	Type of breach	Number of individuals affected	Date reported to ICO/individual	Actions to prevent breach recurring

For help and advice please contact the Information Commissioner's Office.

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

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