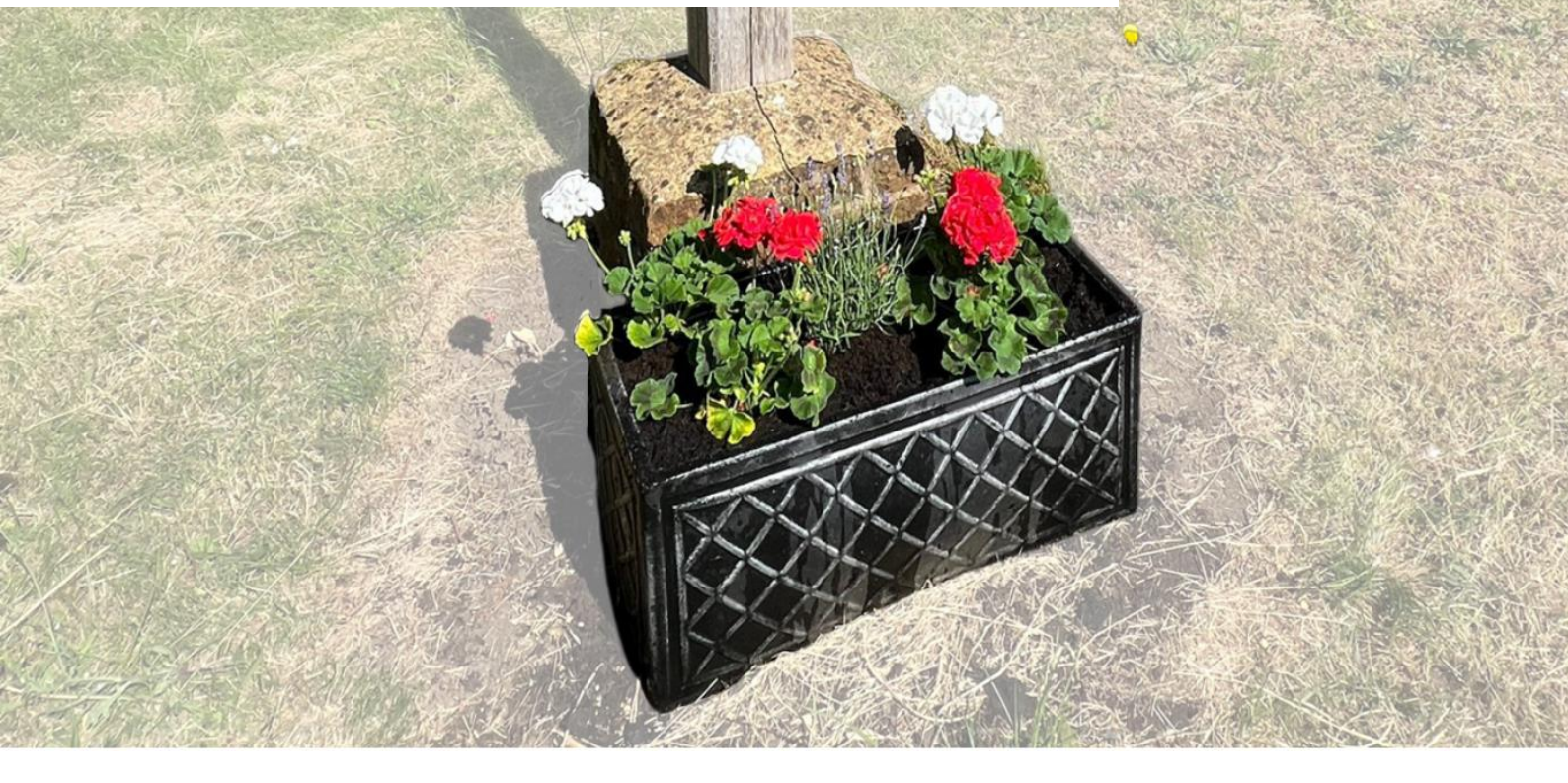
Data Protection & Data Breach Policy

Duston Parish Council



DUSTON PARISH COUNCIL

Document Version Control

Version	Date adopted / Re-adopted	Review By Date	Author
09/23 c	18/05/2023	May 2027	Council

Data Protection Policy

The Data Protection Policy

Duston Parish Council recognises its responsibility to comply with the General Data Protection Regulations (GDPR) 2018 which regulates the use of personal data. This does not have to be sensitive data; it can be as little as a name and address.

General Data Protection Regulations (GDPR)

The GDPR sets out high standards for the handling of personal information and protecting individuals' rights for privacy. It also regulates how personal information can be collected, handled and used. The GDPR applies to anyone holding personal information about people, electronically or on paper. Duston Parish Council has also notified the Information Commissioner that it holds personal data about individuals.

When dealing with personal data, Duston Parish Council staff and members must ensure that:

- **Data is processed fairly, lawfully and in a transparent manner**

This means that personal information should only be collected from individuals if staff have been open and honest about why they want the personal information.

- **Data is processed for specified purposes only**

This means that data is collected for specific, explicit and legitimate purposes only.

- **Data is relevant to what it is needed for**

Data will be monitored so that too much or too little is not kept; only data that is needed should be held.

- **Data is accurate and kept up to date and is not kept longer than it is needed**

Personal data should be accurate, if it is not it should be corrected. Data no longer needed will be shredded or securely disposed of.

- **Data is processed in accordance with the rights of individuals**

Individuals must be informed, upon request, of all the personal information held about them.

- **Data is kept securely**

There should be protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Storing and accessing data

Duston Parish Council recognises its responsibility to be open with people when taking personal details from them. This means that staff must be honest about why they want a particular piece of personal information.

Duston Parish Council may hold personal information about individuals such as their names, addresses, email addresses and telephone numbers. These will be securely kept at the Duston Parish Council Office and are not available for public access. All data stored on the Duston Parish Council Office computers are password protected. Once data is not needed any more, is out of date or has served its use and falls outside the minimum retention time of Councils document retention policy, it will be shredded or securely deleted from the computer.

Duston Parish Council is aware that people have the right to access any personal information that is held about them. Subject Access Requests (SARs) must be submitted in writing (this can be done in hard copy or email). Proof of identity from the person is required. If a person requests to see any data that is being held about them, the SAR response must detail:

- How and to what purpose personal data is processed
- The period Duston Parish Council tend to process it for
- Anyone who has access to the personal data

The response must be sent within 30 days and should be free of charge.

If a SAR includes personal data of other individuals, Duston Parish Council must not disclose the personal information of the other individual. That individuals personal information may either be redacted, or the individual may be contacted to give permission for their information to be shared with the Subject.

Individuals have the right to have their data rectified if it is incorrect, the right to request erasure of the data, the right to request restriction of processing of the data and the right to object to data processing, although rules do apply to those requests.

Confidentiality

Duston Parish Council Members and staff must be aware that when complaints or queries are made, they must remain confidential unless the subject gives permission otherwise. When handling personal data, this must also remain confidential.

Data Breach Policy

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

Duston 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.

Duston 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, Duston Parish Council via the DPO must give reasons for the delay when they report the breach.

When notifying the ICO of a breach, Duston 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 effects.

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

Duston 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 Duston Parish Council

If a data processor (i.e. payroll provider) becomes aware of a personal data breach, it must notify Duston Parish Council without undue delay. It is then Duston 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.

How to Record Data Breaches

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

To report a data breach use the ICO online system:

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