

PRESCOT TOWN COUNCIL



Data Breach Policy

May 2018

Prescot Town Council

Data Breach Policy

The General Data Protection Regulations (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

Prescot Town Council takes the security of personal data seriously, we have a secure cloud server, computers are password protected and hard copy files are kept within a secure office.

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.

Prescot Town 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 the Information Commissioner’s Office (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, Prescot Town Council via the Data Protection Officer (DPO) must give reasons for the delay when they report the breach.

When notifying the ICO of a breach, Prescott Town 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, Prescott Town Council must provide the individual with (ii)-(iv) above along with the nature of the personal data breach using clear and plain language.

Prescot Town 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.

To report a data breach use the ICO online system:

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

Data processors duty to inform Prescott Town Council

If a data processor (i.e. payroll provider) becomes aware of a personal data breach, it must notify Prescott Town Council without undue delay. It is then Prescott Town 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 or the ICO.

Article 33(5) requires Prescot Town Council to document the facts relating to the breach, its effects and the remedial action taken. This is part of the overall obligation to comply with the accountability principle and allows the ICO to verify the organisation's compliance with its notification duties under the GDPR.

As with any security incident, Prescot Town Council should investigate whether the breach was a result of human error or a systemic issue and see how a recurrence can be prevented – whether this is through better processes, further training or other corrective steps.

Data breaches will be recorded on the Prescot Town Council data breach log spreadsheet.