

DATA PROTECTION & DATA BREACH POLICY
(Councillor GDPR check list can be found at the end of this policy)

Introduction

Pitsford Parish Council is fully committed to compliance with the requirements of the Data Protection Act 2018 ("the Act"), which came into force on the 25 May 2018.

The council will follow procedures that ensure that all employees, elected members, contractors, agents, consultants, partners, or other servants of the council who have access to any personal data held by or on behalf of the council, are fully aware of and abide by their duties and responsibilities under the Act.

Statement of policy

To operate efficiently, Pitsford Parish Council must collect and use information about people with whom it works. These may include members of the public, current, past, and prospective employees, clients and customers, and suppliers. In addition, it may be required by law to collect and use information to comply with the requirements of central government. This personal information must be handled and dealt with properly, however it is collected, recorded, and used, and whether it be on paper, in computer records or recorded by any other means there are safeguards within the Act to ensure this.

Pitsford Parish Council regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between the council and those with whom it carries out business. The council will ensure that it treats personal information lawfully and correctly.
To this end the council fully endorses and adheres to the Principles of Data Protection as set out in the Data Protection Act 2018.

The principles of data protection

The Act stipulates that anyone processing personal data must comply with Eight Principles of good practice. These Principles are legally enforceable. The principles require that personal information:

1. Shall be processed fairly and lawfully and shall not be processed unless specific conditions are met.
2. Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Shall be adequate, relevant, and not excessive in relation to the purpose or purposes for which it is processed.
4. Shall be accurate and where necessary, kept up to date.
5. Shall not be kept for longer than is necessary for that purpose or those purposes.

6. Shall be processed in accordance with the rights of data subjects under the Act.
7. Shall be kept secure i.e. protected by an appropriate degree of security.
8. Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of data protection.

The Act provides conditions for the processing of any personal data. It also makes a distinction between personal data and "sensitive" personal data.

Personal data is defined as, data relating to a living individual who can be identified from:

- That data and other information, which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

Sensitive personal data is defined as personal data consisting of information as to:

- Racial or ethnic origin.
- Political opinion.
- Religious or other beliefs.
- Trade union membership.
- Physical or mental health or condition.
- Sexual life.
- Criminal proceedings or convictions.

Handling of personal/sensitive information

Pitsford Parish Council will, through appropriate management and the use of criteria and controls:

- Observe fully conditions regarding the fair collection and use of personal information.
- Meet its legal obligations to specify the purpose for which information is used.
- Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements.
- Ensure the quality of information used.
- Apply checks to determine the length of time information is held.
- Take appropriate measures to safeguard personal information.
- Ensure that the rights of people about whom the information is held can be fully exercised under the Act.

These include:

- The right to be informed that processing is being undertaken.
- The right of access to one's personal information within the statutory 40 days.
- The right to correct, rectify, block, or erase information regarded as wrong information.

Implementation

The Clerk of Pitsford Parish Council is responsible for ensuring adherence with the Data Protection Act.

Notification to the Information Commissioner

The Information Commissioner maintains a public register of data controllers. Pitsford Parish Council is registered as such.

The Data Protection Act 1998 requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence.

The Information Officer will review the Data Protection Register annually, prior to notification to the Information Commissioner.

Any changes to the register must be notified to the Information Commissioner, within 28 days.
To this end, any changes made between reviews will be brought to the attention of the Information Officer immediately.

Appendix 1 – Website and Cookies

Pitsford Parish Council will

1. Seek the *consent of each visitor to their website before a cookie is saved to the visitor's computer.
2. Each cookie will be identified in the Privacy Policy and its purpose explained
3. Visitors, having previously accepted cookies, will be able to withdraw that consent at any time.

*It should be noted that cookies that are essential to make a site work are exempt from consent but not from being detailed in the Privacy Policy.

Last Reviewed: May 2018



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

Pitsford 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.

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

When notifying the ICO of a breach, Pitsford 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, Pitsford Parish Council must provide the individual with (ii)-(iv) above.

Pitsford Parish Council will 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 Pitsford Parish Council

If a data processor (i.e. payroll provider) becomes aware of a personal data breach, it must notify Pitsford Parish Council without undue delay. It is then Pitsford 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 they are reported to individuals. This record will help to identify system failures and should be used 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

To report a data breach use the ICO online system: https://ico.org.uk/for-organisations/report-a-breach/

Adopted: March 11, 2019



GDPR Security Compliance Checklist

All councillors should complete the security checklist below to show compliance. Records should be retained whilst they remain in office.

	Yes/No
Computer is password protected	
Email is password protected	
Mobile devices are password protected	
Flash drives are password protected	
External hard drives are password protected	
Cloud access is password protected	
Hard copy files are held securely	
Anti-virus software is up to date	
No one outside the council has access to your council information	

If you have ticked "No" to any of the above please confirm the date by which you expect to have these measures in place:

Councillor name: _____

Councillor signature: _____

Date: _____