Iwerne Minster Parish Council

Data Protection Policy

(Adopted by resolution April 2018 & July 2019)

Introduction

Iwerne Minster Parish Council needs to gather and use certain information about individuals.

These can include members of the public, suppliers, contractors, employees, Councillors and other people that the Parish Council has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the Council's data protection standards, and to comply with the Law.

This General Data Protection Policy ensures that Iwerne Minster Parish Council:

- Complies with data protection law and follows good practice.
- Protects the rights of staff, general public, contractors and Councillors.
- Is open about how it stores and processes individuals' data.
- Protects itself from the risks of a data breach.

Data protection law

The Data Protection Act (including GDPR) describes how organisations, including Iwerne Minster Parish Council, must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by the following important principles:

- **Lawfulness, fairness and transparency** – Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.
- **Purpose limitation** – Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- **Data minimisation** – Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- **Accuracy** – Personal data shall be accurate and, where necessary, kept up to date.
- **Storage limitation** – Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- **Integrity and confidentiality** – Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- **Accountability** – Iwerne Minster Parish Council shall be responsible for, and be able to demonstrate compliance with data protection.

This policy applies to:

- The Council.
- All staff of Iwerne Minster Parish Council.
- All Councillors of Iwerne Minster Parish Council.

- All contractors, suppliers and other people working on behalf of Iwerne Minster Parish Council.

The policy applies to all data that the Council holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act. This can include:

- Names of individuals.
- Postal addresses.
- Email addresses.
- IP Addresses.
- Telephone numbers.
- Bank Details.
- Any other identifiable information relating to individuals.

Data protection risks

This policy helps to protect Iwerne Minster Parish Council from some very real data security risks, including:

- Breaches of confidentiality, information being given out inappropriately.
- Failing to offer choice, all individuals should be free to choose how the council uses data relating to them.
- Reputational damage, the Parish Council could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or volunteers with Iwerne Minster Parish Council has some responsibility for ensuring data is collected, stored and handled appropriately.

The Clerk and Councillors that handle personal data must ensure that it is handled and processed in line with this policy and data protection principles.

The following are the key areas of responsibility:

- The Chairman is ultimately responsible for ensuring that Iwerne Minster Parish Council meets its legal obligations.
- The Data Protection Representative, is responsible for:
    - Keeping the Council updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging data protection training and advice for the people covered by this policy.
    - Handling data protection questions from staff and anyone else covered by this policy.
    - Dealing with requests from individuals to see the data Iwerne Minster Parish Council holds about them.
    - Checking and approving any contracts or agreements with third parties that may handle the Council's sensitive data.
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - Performing regular checks and scans to ensure security hardware and software is functioning properly.
    - Evaluating any third-party services the Council is considering using to store or process data. For instance, cloud computing services.
    - Approving any data protection statements attached to communications such as emails and letters.

General staff guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally.
- Employees and Councillors should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the Council or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.

Data storage

These rules describe how and where data should be safely stored.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- When data is no longer required, it can be destroyed or preserved (using the Parish and Town Council Guidance on retention, disposal guide).
- Employees and Councillors should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.
- When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts.
- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the Council's standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.

Data use

Personal data is of no value to Iwerne Minster Parish Council.

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. In particular, it should never be sent by email, unless secure connection can be guaranteed.
- Data must be encrypted before being transferred electronically.

- Personal data should never be transferred outside of the UK unless guidance to do so has been provided.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

Data accuracy

The law requires Iwerne Minster Parish Council to take reasonable steps to ensure data is kept accurate and up to date.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- Data should be updated as inaccuracies are discovered.

Subject access requests

All individuals who are the subject of personal data held by Iwerne Minster Parish Council are entitled to:

- Ask what information the Council holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the Council is meeting its data protection obligations.

If an individual contacts the Council requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to Iwerne Minster Parish Council at iwerneminster@dorset-aptc.gov.uk.

Iwerne Minster Parish Council will consider the reality of the request and it is felt relevant the Council will aim to provide the relevant data within 30 working days.

Iwerne Minster Parish Council must verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons.

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Iwerne Minster Parish Council will disclose requested data. However, the Council will ensure the request is legitimate, seeking assistance from the Councils legal advisers where necessary.

Providing information

Iwerne Minster Parish Council aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used.
- How to exercise their rights.

This is available on request to the Council.

Roles defined by the GDPR

Data Processing Agreements – processors may only process personal data on behalf of a controller where a written contract is in place which imposes a number of mandatory terms on the data processor, as set out in the GDPR.

Controller instructions – processors may only process personal data in accordance with the instructions of the controller.

Accountability – processors must maintain records of data processing activities and make these available to the supervisory authority on request. Iwerne Minster Parish Council is working with DAPTC to designate a data protection officer.

Iwerne Minster Parish Council are registered with ICO (Information Commissioners Office)

Note:

See also Iwerne Minster Parish Council's Privacy Notice.