Pauntley Parish Council

Data Protection & Information Security Policy

(This document is to be read in association with Pauntley Parish Council's Privacy Policies and Subject Access Request Policy)

Why this policy exists

This data protection & information security policy seeks to ensure that Pauntley Parish Council:

- Compiles with the General Data Protection Regulation (GDPR) and follows good practice
- Protects the rights of councillors, staff, volunteers, and partners
- Is open and transparent about how its stores and processes individuals' data
- Protects itself from the risks of a data breach
- Protects itself from reputational risk
- Protect the information it stores about others

The type of data this policy is about

It applies to all data that the Council holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names of individuals
- Postal addressees
- Email address
- Telephone numbers
- Plus any other information relating to individuals

Data protection law

GDPR 2018 describes how organisations – including Pauntley 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.

GDPR is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary

6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside of the European Union (EU), unless that country or territory also ensures an adequate level of protection

Article 5(2) requires that the controllers shall be responsible for and be able to demonstrate compliance with these principles.

Responsibilities

All councillors and those who work and volunteer for or with Pauntley Parish Council has a responsibility for ensuring data is collected, stored and handled appropriately.

Each person that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

Pauntley Parish Council is ultimately responsible for ensuring that it meets its legal obligations. However, individuals within the council will also have specific responsibilities as those outlined below.

- The Clerk is responsible for:
  - Keeping the council updated about data protection responsibilities, risks and issues, including notification of any breaches
  - Reviewing all data protection procedures and related policies
  - Arranging data protection training and advice for the people covered by this policy
  - Handling data protection questions from councillors and anyone else covered by this policy
  - Dealing with requests from individuals to see the data Pauntley Parish Council holds about them (also called 'subject access requests')
  - Checking and approving any contracts or agreements with third parties that may handle Pauntley Parish 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 foundation is considering using to store or process data. For instance, cloud computing services, remote backup services
  - Ensuring marketing initiatives abide by data protection principles
  - Approving any data protection statements attached to communications such as emails
  - Liaising with the Chairman to address any data protection queries from journalists or media outlets like newspapers and magazines

- Councillors are responsible for:
  - Adopting the relevant policies and procedures to ensure that the Council is complying with the law
  - Managing and working with data in accordance with this policy

- Supporting the Clerk to ensure they are equipped to help the Council meet its statutory responsibilities

General guidelines

- The only people able to access data covered by this policy should be those who need it to carry out their duties
- Data should not be shared informally
- Pauntley Parish Council will provide training to all councillors and employees to help them understand their responsibilities when handling data
- Employees and councillors should keep all data secure, by taking sensible precautions and following the guidelines below
- Strong passwords must be used, and they should never be shared
- Personal data should not be disclosed to unauthorised people, either within Pauntley Parish Council or externally
- Data should be regularly reviewed and updated. If no longer required, it should be deleted and disposed of
- Councillors and staff should request help from the Clerk, Gloucestershire Association of Parish & Town Councils or the Information Commissioner's Office if they are unsure about any aspects of data protection.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Clerk.

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:

- Employees and councillors should make sure paper and printouts are not left where unauthorised people could see them, like on a printer or on their desk at the end of their working day (visible to cleaners/contractors)
- Data printouts should be disposed of securely when no longer required via the secure shredding bin
- 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 colleagues

- If data is stored on removable media (i.e. CD, DVD, memory stick), these should be kept locked away securely when not being used.

- Data should only be stored on Pauntley Parish Council's data storage devices and should only be uploaded to an approved cloud computing system.

- Data should be backed up frequently. Those backups should be tested regularly

- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones unless the mobile device is encrypted.

- All computers containing data should be protected by approved security software and firewalls

Data use

Personal data is of no value to Pauntley Parish Council unless the organisation can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees and councillors should ensure the screens of their computers are locked when left unattended

- Personal data should only be accessible from Pauntley Parish Council's recognised places of business

Data accuracy

The law requires Pauntley Parish Council to take all reasonable steps to ensure data is kept accurate and up to date, therefore, to help us achieve this:

- Data will be held in as few places as necessary. Staff and councillors should not create any unnecessary additional data sets.
- Staff and councillors will take every opportunity to ensure data is up to date.
- Pauntley Parish Council will make it easy for data subjects to update the information it holds about them
- Data will be updated as inaccuracies are discovered. For instance, if a contact can no longer be reached on their stored contact number or email, it will be removed from the database.

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

Subject access requests

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

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

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

Subject access requests from individuals can be made by email, addressed to the clerk at pauntleypc@gmail.com. The clerk will aim to provide the relevant data within one month of the date of the request.

The clerk will always verify the identity of anyone making a subject access request before handing over any information.

The Council has a Subject Access Request policy that also outlines its procedures in more detail. This policy can be found on the Council's website at www.Pauntley.org.uk OR can be requested from the Clerk at pauntleypc@gmail.com

When Pauntley Parish Council can withhold information

There are some situations when organisations are allowed to withhold information, e.g. if the information's about:

- the prevention, detection or investigation of a crime
- national security or the armed forces
- the assessment or collection of tax
- judicial or ministerial appointments

An organisation doesn't have to say why they're withholding information.

Disclosing data for other reasons

In certain circumstances, the GDPR allows personal data to be disclosed if required to do so by law without the consent of the data subject.

Under these circumstances, Pauntley Parish Council will disclose requested data. However, the clerk will ensure the request is legitimate, seeking assistance from relevant and appropriate authorities where necessary.

Pauntley Parish Council will not share Data for any other reason than mentioned above.

Providing information

Pauntley 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

To these lines, Pauntley Parish Council has privacy policies, setting out how it uses data relating to individuals. A copy of the privacy policies is available on the Pauntley Parish Council website.

Personal data breaches

The ICO defines personal data breaches as:

'….. a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.'

What you must do if there is a personal data breach

If any councillor or member of staff suspects or knows of a personal data breach it must be reported immediately to the Clerk with details of:

- what has happened
- when and how you found out about the breach
- the people that have been or may be affected by the breach

The Clerk will record the incident and take appropriate action that will include reviewing the processes and procedures to minimise the risk of such an incident happening again, whilst also looking at ways in which any harm or potential harm that may result from the incident could be reduced. The Clerk may also conclude, with or without the advice of relevant others, that the risk to an individual meets the legal requirement that the incident must be reported to the Information Commissioner's Office.

All staff and councillors associated with Pauntley Parish Council are required to familiarise themselves with the council's Privacy Policy.