GENERAL DATA PROTECTION REGULATION POLICY

This policy updates the Parish Council’s current Data Protection Policy and procedures to include the additional requirements of GDPR which will apply in the UK from 25th May 2018. The Government has confirmed that despite the UK leaving the EU, GDPR will still be a legal requirement probably via the Great Repeal Bill.

This policy explains the duties and responsibilities of the Parish Council and identifies the means by which the Parish Council will meet its obligations.

MINIMISING RISK AND IDENTIFYING ROLES

GDPR requires that everyone within the Parish Council must understand the implications of GDPR and that roles and duties must be assigned. The Parish Council is the Data Controller and is the Data Protection Officer (DPO).

The Parish Council is the Data Controller because we hold data on Parish Councillors, employee/s and sometimes residents.

Personal data must be processed lawfully, fairly and transparently; collected for specified, explicit and legitimate purposes, be adequate, relevant and limited to what is necessary for processing; be accurate and kept up to date; be kept only for so long as is necessary for processing; and be processed in a manner that ensures its security.

Information handling is a high/medium risk to the Parish Council and will be included in the Parish Council’s Risk Assessment. Such risks can be minimised by undertaking an Information Audit; issuing privacy statements; minimising who holds information, and the safe disposal of information and training.

GDPR requires continued care by the Data Protection Officer and Parish Councillors in the sharing of information about individuals, whether as a hard copy or electronically. A breach could result in a fine and a payment for compensation.

THE SIX DATA PROTECTION PRINCIPLES

1. LAWFULNESS, FAIRNESS & TRANSPARENCY

Lawfulness: Processing must meet the tests described in GDPR;

Fairness: What is processed must match up with how it has been described; and Transparency: Tell the subject what data processing will be done.

1. PURPOSE LIMITATION

This will be contained in the Parish Council’s Privacy Notice, ie telling people why we need their data when we collect it from them, what we will do with it, who we will share it with and how long we will keep it.

1. DATA MINIMISATION

This must be adequate, relevant, and limited to what is necessary.

1. ACCURACY

Up to date and accurate. If inaccurate, correct and delete without delay.

1. STORAGE LIMITATION

Data must not be kept longer than is necessary or legally required.

1. INTEGRITY & CONFIDENTIALITY

Data must be kept physically and electronically securely.

THE SIX LEGAL PURPOSES FOR THE LAWFUL PROCESSING OF DATE

1. CONSENT

This is the usual basis for processing data, with burden of proof higher under GDPR.

Consent means ‘freely given specific and informed indication of wishes by which data subject signifies agreement to their personal data being processed’.

Consent is not freely given if there is no real choice or refusal or withdrawing consent will cause detriment. Withdrawing consent should be as easy as giving consent. The burden of proof is on the Data Controller (The Parish Council) to prove consent was given. Consents should be regularly reviewed and updated. (ICO recommends every two years).

1. PERFORMANCE OF CONTRACT

This means the collection and processing of data to provide the service.

1. COMPLIANCE WITH LEGAL OBLIGATION

Processing is necessary for compliance with a legal obligation to which the controller is subject.

1. VITAL INTERESTS OF DATA SUBJECT

For example, monitoring epidemics, and humanitarian emergencies.

1. PUBLIC INTEREST

For example, the use of personal data for the collection of income tax.

1. LEGITIMATE INTERESTS OF DATA CONTROLLER

For example, for the prevention of fraud.

ENHANCED RIGHTS FOR ALL INDIVIDUALS

All individuals who have dealings with the Parish Council have these rights and the Parish Council needs to take account of these rights.

REQUESTS FOR INFORMATION (SUBJECT ACCESS REQUESTS)

Under the GDPR a data controller may not charge for dealing with a request for access to personal data (a subject access request), the Parish Council must reply promptly and, in any event, within one month (for complex, or numerous, requests this period can be extended by a further two months). There is discretion to charge a reasonable fee, or refuse to comply if the request is unfounded, or excessive, but the data controller bears the burden of proving the request was unfounded or excessive. Third Parties can ask for information but must still prove they have consent, or justify why it is appropriate, as they do now.

TRANSPARENCY

People should know whether they are obliged to provide their personal data and what the potential consequences are. This needs to be clear at the point of collecting the data.

RECTIFICATION

The right to have inaccurate personal data corrected. If inaccurate data has been shared there is an obligation to inform any recipients of the correction unless this is impossible or would involve disproportionate effort.

ERASURE (THE RIGHT TO BE FORGOTTEN)

This is not an absolute right and it does not apply if there is a lawful reason for continued processing. This might be a factor, for example where the Parish Council has employment records and someone requests that details of a grievance, or a disciplinary matter, be removed.

RESTRICTION OF PROCESSING

Where there is a dispute about the processing of the data then affected personal data may only be processed with the data subject’s consent, for establishing or defending legal claims, for the protection of another natural or legal persons’s rights or for reasons of important public interest. This restriction continues until the dispute is resolved.

DATA PORTABILITY

This allows a data subject to instruct a data controller to transmit their personal data to another controller where it is technically feasible to do so. There is no obligation to maintain, or adopt, technically incompatible systems.

OBJECTION TO PROCESSING

A data subject can object to the processing of their data and a data controller must respond within one month (within a potential two month extension for complex, or numerous, requests). Processing includes profiling for the public interest, for direct marketing and for historical research or statistical purposes. Other than direct marketing the request is subject to the application of the public interest test.

DATA PROTECTION PRINCIPLE SIX

INTEGRITY & CONFIDENTIALITY – KEPING PERSONAL DATA SECURE

Keeping personal data secure means keeping IT systems secure. For example, strong passwords, regular back-ups, keeping software updated, and applying patches as soon as possible; and covers encryption, anonymising data and having guidance for the storage of Parish Council business tablets or phones, and having a Parish Council email address.

IMMEDIATE IMPACT OF GDPR ON THE PARISH COUNCIL

1. Notification is abolished. The Parish Council needs to continue to maintain the record of processing what it already has and keep it updated.
2. Appoint a Data Protection Officer, who must have:

* Appropriate expertise;
* Be able to report to the Parish Council;
* Be able to operate independently
* Cannot be dismissed for carrying out their role properly.

In a Small Parish Council the tasks will be:

* Dealing with subject access requests and ‘right to be forgotten’ requests;
* Reporting data breaches to ICO and affected data subjects;
* Implementing and updating policies and procedures;
* Dealing with enquiries and complaints from data subjects.

1. The need to review policies on data security, retention and responding to requests for information because they all should work together. This includes a clear process (that everyone is aware of) for identifying a breach of data security and deciding whether it needs to be reported to the ICO.
2. Put in place a Privacy Notice and to ensure the Parish Council has appropriate privacy wording whenever personal data is collected.
3. Check IT security – regular back-ups undertaken, and updates need to be applied as soon as available. Patches issued to deal with hoes in security need to applied as appropriate.
4. Check explicit consent is being obtained to use personal data and do not rely on implied consent, pre-ticked boxes or inactivity.
5. When considering using cloud services look for the Cloud Infrastructure Service Providers in European Code of Conduct.

An Information Audit will need to be reviewed annually. Or when services or projects change.

This policy will be reviewed annually or when further advice is issued by the ICO.

All employees, volunteers and Councillors are expected to comply with this policy at all times to protect privacy, confidentiality and the interests of Havenstreet and Ashey Parish Council.

See following twelve steps for Havenstreet and Ashey Parish Council to implement.

1. Awareness

Everyone in the Parish Council must be aware of what is happening.

1. INFORMATION THE PARISH COUNCIL HOLDS (INFORMATION AUDIT)

The Parish Council needs to check what information it holds (and why) and decide whether it needs to keep it.

1. COMMUNICATING PRIVACY INFORMATION

The Parish Council needs to tell people why it is collecting their data, what it will be used for, who it will share it with and how long it will be kept for, and this needs to be done every time data is collected.

1. INDIVIDUAL’S RIGHTS

The Parish Council needs to ensure its policy makes clear the rights individuals have to see their information, correct it, delete it or transfer it.

1. SUBJECT ACCESS REQUESTS

The Parish Council needs to ensure this policy is easily available and easy to understand.

1. LAWFUL BASIS FOR PROCESSING INFORMATION

The Parish Council needs to ensure they are processing data by consent.

1. CONSENT

Pre-ticked boxes are no longer enough. The Parish Council needs to receive explicit and informed consent.

1. CHILDREN

Verification of age and seeking parental consent if necessary. Thirteen will probably be the UK age of consent for this purpose (that is children aged thirteen and over are generally deemed able to consent to the processing of their own personal data).

1. DATA BREACHES

The Parish Council needs to have a process for identifying breaches and reporting them.

1. DATA PROTECTION BY DESIGN & DATA IMPACT ASSESSMENTS

Systems and policies should have safeguards for personal data built in.

1. DATA PROTECTION OFFICER

Local Authorities have to appoint a Data Protection Officer. The Parish Council needs to ensure the Council/Councillors understand the duties and responsibilities.

1. INTERNATIONAL TRANSFER

If the Parish Council were to use ‘cloud services’ this could result in an international transfer.