Microshade VSM

Local Council Community Cloud

BISHOPSTONE PARISH COUNCIL

GDPR Audit Report May 2018 Version One

General Data Protection Audit Report and Action Plan for Bishopstone Parish Council – May 2018

CONTENTS

1. Introduction…… 1

2. Identification of Personal Data Held……. 1

3. Collection of Personal Data……. 3

4. Record Management…….. 6

5. Information Sharing……... 8

6. Conclusion……... 8

1. INTRODUCTION

1.1 The General Data Protection Regulations (GDPR) will replace the Data Protection Act and will apply in the United Kingdom from 25th May 2018. GDPR introduces a number of new requirements, including changes to privacy notices, consent and requests to view personal data. These requirements are encapsulated in a new Data Protection Bill currently being passed in Parliament.

1.2 The Data Protection Bill can be reviewed in its current form by following the link https://publications.parliament.uk/pa/bills/lbill/2017-2019/0066/lbill_2017-20190066_en_1.htm

1.3 This audit aims to review the existing mechanisms within your organisation for processing personal data. At the end of the audit there will be some actions that you will need to carry out to ensure that you are compliant by 25th May 2018.

1.4 The audit is in 4 parts:

- Identification of what personal data is held
- Collection of personal data
- Records management
- Information sharing

1.5 Some of the information will be used to create an information asset register showing what information the council holds, so that you can demonstrate that you know where your personal data is held.

1.6 An Action Plan has also been developed to identify the initial findings of the audit and to outline actions that need to be taken so that the Council becomes fully compliant with GDPR, and to ensure that the potential of a data breach is reduced.

2. IDENTIFICATION OF PERSONAL DATA HELD

2.1 In order to carry out its functions and deliver its services Bishopstone Parish Council does collect personal data.

2.2 Personal data is collected for the following reasons within the Parish Council:

- Finance & Administration;
- Democratic services;
- Payroll.

2.3 The Clerk works from home and all data, including personal data information, is held at the Clerk's home, Bankcroft, Monkland, Herefordshire HR6 9DB (Tel: 01568 720092).

2.4 The table below is an overview of the Parish Council's infrastructure and areas that generates the requirement to collect personal data:

Service Area	Description
Brief description of services delivered	• Newsletter • Website • Planning consultees
Description of sites	• None
Councillors	10
Staff	Clerk to the Council
Volunteers	None
Details of current contractors and service providers	• Mark Milmore (website via HALC); • Internal Auditor.

2.5 Classes of Records are descriptions of all records and information created, captured and maintained by the Parish Council as evidence of the administration of a particular program, activity and sub-activity specific to the Parish Council. The following classes of records are collected by the Parish Council:

- Employee personal information;
- Councillor personal information;
- Financial transactions (internet banking)
- Democratic services
- Residents;
- Ad-hoc contractors and other service providers;
- Complainants.

2.6 The Parish Council keeps both electronic and paper based records in the following formats:

Paper:	**Electronic:**
Loose papers	Word
Loose papers in folder	Excel
Cardboard files	Emails
Ring binders	HMRC PAYE software
	Finance software

2.7 The following personal data is collected by the Parish Council:

Full Name	Contact Details (e.g. postcode, address, phone number, e-mail)
References (HR, contracts) (will be collected in the future)	Financial details (bank details, earnings)
Employment details	Goods or services provided
Disability status (in future)	Physical/mental health (in future)
Medical information (in future)	Photographs (newsletter)

Personal data is collected as part of the following services:

- General administration (contact is encouraged via the website)
- Councillors (democratic services)

- Newsletter production
- Volunteers
- Community organisations
- Events
- Public consultations
- Payroll
- Finance/accounts

2.8 Biometric data includes technology that identifies employees based on physical characteristics, such as fingerprints, iris colour, or voice recognition. The most common use of biometric data at present is fingerprints (smartphone access) and voice recognition. The Parish Council does not collect any of this information.

2.10 Personal information is updated on an ad-hoc basic and there is no procedure in place to update information across the Parish Council on a regular basis.

No privacy notices included at present.

Action:

- To include privacy notices on all forms and provide an opportunity, where applicable, for the person to give their explicit consent.
- To ensure that the privacy notice and statement is clear, transparent and easy to understand;
- To request all Councillors to complete the new privacy notice.
- To update the website with Data Protection policies, general privacy notice and other information.
- To ensure that a Data Protection Policy and a Data Breach Procedure has been adopted by Council.
- To ensure that all web forms have the correct GDPR privacy notices and policies uploaded.
- To check and amend the current retention policy as required.
- To develop a deletion, erasure and updating/correcting information procedure.
- To ensure that all contractors and organisations are observing the new GDPR requirements.

2.11 The Parish Council does not provide any services that require or use automated decision making and it does not undertake customer profiling.

3. COLLECTION OF PERSONAL DATA

3.1 The Parish Council collects personal data identified for the following purposes:

Class of Record	**Purpose**
Personnel Records	• To keep a record of all staff employed to services on behalf of the Parish Council; • Contract requirement

	• Health & Safety; • Insurance; • Legal requirement.
Councillor personal information	• To deliver democratic representation as part of the LGA 1972; • To provide open and transparent governance; • Health & Safety; • Insurance
Contractor information	• To keep a record of all contractors providing services for and on behalf of the Parish Council; • To pay outstanding accounts; • Contract requirement; • Health & Safety; • Insurance; • Legal requirement.
Residents	• Service delivery; • Addressing planning questions; • Public consultations; • Addressing general enquiries; • Annual Parish Meeting; • Improving, developing and addressing service issues; • Improving the Parish Council.
Complainants	• Service delivery; • Improving, developing and addressing service issues; • Improving the Parish Council.
Mailing lists	• To help develop, deliver and assess services; • To keep people informed of what is going on in the Parish.
Volunteers	• To keep a record of all volunteers providing voluntary services to enable a range of services to be delivered; • Contract requirement; • Health & Safety; • Insurance; • Legal requirement.

3.2 The six lawful basis for collecting information are as follows. At least one of these must apply whenever the Parish Council processes personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

3.3 The legal basis for collecting the personal information is as follows:

Class of Record	**Legal Basis**
Personnel Records	• Contractual necessity; • Compliance with legal obligation; • Vital Interests.
Councillor personal information	• Contractual necessity; • Compliance with legal obligation.
Contractor information	• Contractual necessity; • Compliance with legal obligation.
Residents	• Explicit Consent.
Complainants	• Compliance with legal obligation. • Public Interest.
Volunteers	• Explicit Consent
Newsletter	• Explicit Consent

New privacy notices should contain the legal basis for the Parish Council collecting information.

3.4 The following privacy notices will need to be developed and sent out to the relevant recipients to ensure GDPR compliance:

- General contact and personal data usage Privacy Notice;
- Volunteers Privacy Notice;
- Councillors Privacy Notice;
- Employee Privacy Notice;
- Complainants Privacy Notice;
- General Mailing List Privacy Notice;

- Contractor Privacy Notice.

3.5 The following sources provide information:

Source of Information	Provider
The person to whom the information relates	• The Data Subject
Another source or organisation	• Complaints received and forwarded to the Clerk for action • HALC • Herefordshire Council

3.6 Information is transferred in a variety of ways when received:

Information Receipt	Recording Method/Transfer
Telephone (Verbal)	• Information noted and then retained in order to action.
Email (Electronic)	• Information received by email is forwarded on either to Councillors for action or retained by the Clerk to action.
Internet/web based information	• Information received by email is actioned by the Clerk;
Letter (Paper/Hard copy)	• Information received by mail is dealt with by the Clerk and retained for future reference in case of query.
Verbally (face to face)	• Information received through face to face contact, via Councillors etc; • Information/issue then recorded then transferred physically or electronically to Clerk.

- A new Privacy Notice to be included on replies indicating legal reason for retaining data and the retention period;
- An email response privacy notice to be included on emails outlining the Town Council's commitment to GDPR;
- Correspondence should be replied to by the Parish Council acknowledging receipt and including the privacy notice outlining how personal data will be processed.

3.7 Consent is sought and obtained verbally, electronically and signed correspondence. There is currently no consent privacy notice in place.

3.8 Verification of individual's ages is not sought by the Parish Council.

4. RECORD MANAGEMENT

4.1 The Clerk works from home and all records are stored here. The Parish Council stores a range of records, some of which contain sensitive personal information.

Location	Type of Records Stored
Clerk's Home	• Payroll data; • Employee records; • Councillor information; • Contractor information; • Minutes, agendas; • Financial records; • Tenders; • Correspondence; • Complaints.

4.2 Records are stored in a number of formats. Hard copy record storage is dealt with under 4.1 above but other record storage is outlined below:

Type of Storage	Location of Storage
Electronic storage	• Internal hard drive (C drive) • Email account

4.3 Access to records is based on the sensitivity of the records being stored.

Record	Accessibility
General Council records	• Clerk has access to all records in either hard copy or electronically.
Employment records	• Parish Clerk and the Chair, if required.
Accounts records	• Parish Clerk; • General account information is available to all who may request it, subject to legislative restrictions.

4.4 The following electronic access controls are in place. There is limited access:
- Password protected computer access.

4.5 There are no following manual access controls in place but there is limited access to the Clerk's Office (based at home)

4.6 The following manual storage systems are in place:
- Open shelving.

• Carry out a review of the data storage location to ensure that access by unauthorised personnel is reduced to a minimum. Actions may include

additional locked storage cabinets and the destruction of sensitive information no longer required.

4.7 The Parish Council does not have a Retention Policy in place.

4.8 There is no formal procedure in place for correcting or erasing data but the Parish Council follows the NALC guidelines contained within the Retention policy.

- Carry out a review of disposal, erasing and correcting data processes and procedures;
- Develop a formal policy to deal with the updating of records and the deleting of records in line with the Council's retention policy;
- Ensure that contractors and agencies are GDPR compliant in this area.

4.9 Council emails are currently stored at a Hotmail account. Hotmail has now ceased to exist as an email address and new accounts are normally @live.co.uk. It is advised that a specific email provider is requested to host emails in the UK or EU.

4.10 Emails are stored in project files within the email account. A procedure to delete old emails may need to be considered.

- Review email management and retention;
- Include a process to delete emails that contain sensitive information and do not have consent for retention.

5. INFORMATION SHARING

5.1 The Parish Council does not share any personal data with any other organisations.

5.2 There are therefore no data sharing agreements in place.

6. CONCLUSION

6.1 The Information Commissioner's Office has acknowledged that many organisations will not be fully compliant with the new GDPR regulations by 25th May 2018. However, every organisation affected by the new legislation, which is still going through Parliament and has not been finalised, should evidence that it has made a start.

6.2 Following the Data Audit which has been carried out, an Action Plan has been developed and will need to be implemented. This is a separate document from the Data Audit Report. The timescale for the implementation of the Action Plan needs to be reviewed and discussed prior to formal adoption.

6.3 The Parish Council has commenced its preparations to get ready for the General Data Protection Regulations. By commencing the implementation of

the recommendations contained within the Action Plan it will begin to work towards GDPR compliance.

6.4 The Action Plan prioritises the steps required to become fully GDPR compliant. However, the Parish Council will need to keep GDPR under review on a proactive basis, and put in place systems to assess compliance in the future, such as Data Privacy Impact Assessments (DPIA) for new projects.

6.5 The appendices provided to the Parish Council include a revised Data Protection Policy for the Council, a revised Retention Policy and template Privacy Notices. These should be internally reviewed and updated to reflect the processes and protocols currently adopted by the Parish Council.

6.6 The following actions should be undertaken prior to 25th May 2018:

- Adopt the Data Audit;
- Revise and commence implementation of the Action Plan and recommendations within the Data Audit;
- Consider the formal appointment of a Data Protection Officer as it is considered Best Practice and provides a source of advice relating to GDPR on an on-going basis;
- Revise the relevant forms to include the amended versions of the template privacy notices provided;
- Adopt a Data Protection Policy and upload it and other relevant documentation on to the Council's website;
- Adopt a Data Breach Policy and procedure;
- Note the requirement to carry out Data Protection Impact Assessments for all new contracts and services (this is not retrospective);
- Carry out training for staff and Councillors.