West Harptree Parish Council Report

The General Data Protection Regulation 2016 (GDPR)

1. Outline of the legislation and regulatory framework

The GDPR 2016 came into force on 25th May 2018, and arises from the Data Protection Act 1998.

The GDPR requires West Harptree Parish Council (the PC) to have a Privacy Notice; agreements for sharing information with partners; and procedures for responding to data protection subject access requests.

NALC has advised that these requirements can be achieved through a Data Protection Policy, which documents the PC's lawful basis for processing personal data.

Personal data is information relating to a living individual who can be recognised from that data.

Under the GDPR, personal data must be:

a. processed fairly, lawfully and in a transparent manner in relation to the data subject;

b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d. accurate and, where necessary, kept up to date;

e. kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

f. 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.

Under the GDPR, the Parish Council and Clerk are **Data Controllers**; the Parish Council's contractors such as the website provider may be **Data Processors**; and any person whose data is held is a **Data Subject**. The GDPR does not define a parish council as a public authority therefore does not require it to appoint a Data Protection Officer.

A Data Controller must have a legitimate reason for processing personal data, and must be able to show that the Data Subject has freely given specific, informed, and unambiguous consent for each purpose for which the data is being processed. The Data Subject also has the right to withdraw consent. In the case of a child, consent must be obtained from the parents.

A Data Controller must provide a Data Subject with the following information in a Privacy Notice:

a. the identity and the contact details of the data controller and, if any, of the controller's representative and, if any, the data protection officer;

b. the purpose(s) of the processing;

c. the categories of personal data concerned;

d. the recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular recipients in third countries or international organisations;

e. where possible, the envisaged period for which the personal data will be stored or, if not possible, the criteria used to determine that period;

f. the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

g. the right to lodge a complaint with the ICO and where the personal data is not collected from the Data Subject, any available information as to its source.

A Data Controller is required to oblige Data Processors to:

a. process the personal data only on the documented instructions of the controller;

b. comply with security obligations equivalent to those imposed on the controller under Article 32 of the GDPR;

c. only employ staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;

d. enlist a sub-processor only with the prior permission of the controller;

e. assist the controller in carrying out its obligations with regard to requests by data subjects to exercise their rights under Chapter III of the GDPR (including the right to transparency and information, the data subject access right, the right to rectification and erasure, the right to the restriction of processing, the right to data portability and the right to object to processing);

f. assist the data controller in carrying out its data security obligations under Articles 32 to 36 of the GDPR (Article 28).

The requirement for a Data Controller to maintain a written record of processing activities only applies to organisations employing more than 250 people, unless the data processed is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data.

A Data Controller must keep a record of all personal data breaches, and in certain circumstances report any personal data breaches to the ICO and the affected individual without delay (and within 72 hours).

A Data Processor must also inform a Data Controller of any personal data breach without delay.

The ICO may fine a Data Controller for serious breaches. Examples of personal data breaches include

- access by an unauthorised third party;
- deliberate or accidental action or inaction by a Data Controller or Processor;
- sending personal data to the wrong recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

The Freedom of Information Act 2000 covers all recorded information held by the PC (with limited exemptions). However, personal information should be deleted (redacted) from any information provided. A request for information from a member of the public does not have to specify that it is made under this Act.

The Local Audit & Accountability Act 2014 gives members of the public the right to inspect the PC's accounts and supporting documents. The latter may contain personal data as defined by the GDPR.

The Transparency Code for Smaller Authorities 2014 requires the PC to publish specified details of its meetings, financial management, audit, assets and governance.

2. West Harptree Parish Council – data in general

The PC does not collect, hold or process any personal information defined as a protected characteristic in the Equality Act 2010 (ie relating to age; disability; gender reassignment; marriage and civil partnership; pregnancy and maternity; race; religion or belief; or sex). The PC might be provided with such data if it supported a parishioner in a complaint to a service provider, in which case the data would be supplied by the data subject, would only be used in accordance with their instructions, and would be destroyed once the matter had been resolved.

The PC does not provide or exchange data containing the personal details of any individual without the express consent of the individual concerned.

The PC may hold photographs of volunteers. Permission is not needed to take and publish a photograph of a person in a public place.

The PC does not collect or process personal data, except incidentally in the normal course of business. Most of this data comprises names, postal and email addresses, telephone numbers and correspondence in the form of emails and documents. Some of this information is already publicly available through directories, publications and other organisations.

The PC does not hold any personal financial information, except in the case of the Clerk who is a salaried employee. The PC holds cancelled cheques for audit purposes: these bear the account details of the payee.

Receipts and payments accounts are kept in manual form and published and the PC is considering using internet banking.

The PC's website is controlled by the Chairman and Clerk and contains only public information. The flow of information is from the PC to the website to the public and a contact formis used to direct messages from the website back to the Clerk or Council. It is not known whether the website uses cookies. The website collects user statistics which are likely to be anonymised.

The PC does not offer or undertake any commercial activity, and does not hold or process any personal financial information relating to members of the public.

Emails sent and received between Councillors and the Parish Clerk, members of the public, and other organisations are in text format written form and open to scrutiny. The PC does not use SMS text messaging.

All Parish Councillors have personal email addresses which are not shared by others, and are protected by robust anti-virus and anti-malware internet security systems which are kept up to date. At present Councillors use personal email addresses for PC business.

The PC employs a third party (Data Processor) to host and update the web site

3. West Harptree Parish Council – data mapping

a) Stakeholders, circulation and interested parties

Members of the public; parishioners; parish, district and county councillors; members of parliament; national and local government departments and organisations; charities, associations; service providers; contractors.

b) Types of data handled

Emails and attachments including images; paper documents; notes of meetings and conversations.

c) Direction of data

Inwards to the Clerk; outwards to appropriate parties and the parish council website; some data retained and/or processed for statutory records. Personal information is never sent out without consent.

d) Data files inward

All aspects of parish council business from individuals and contractors to organisations of all kinds and sizes. The Clerk is likely to receive false invoices and phishing emails.

e) Data files outward

All aspects of parish council business from individuals and contractors to organisations of all kinds and sizes.

f) Parish Council website

Is managed by the Chairman the Clerk and a volunteer computer expert. Data flow is from the Parish Clerk to the website. The website does not allow users to edit or input any information save that it does include a contact / enquiry form.

g) Commercial and financial activity

The Parish Council does not use internet banking, and does not carry out any commercial activities. The Parish Councils accounts and supporting documents are published and open to public examination as required by law.

h) Consent

West Harptree Parish Council ignores all anonymous communications. The Parish Council assumes that any individual who communicates with the Parish Council will expect a reply, and has implicitly consented to their contact details being held, at least until the matter has been closed.

i) File retention and deletion

Files are currently deleted some time after the matter in question has been dealt with, or when they are no longer required for consultation under the current publication scheme.

j) Right to be forgotten

Any person can apply at any time to have their own details removed from Parish Council records. It is not clear how this right can be complied with in the case of photographs which have been taken with permission and then published.

4. Risk assessment

The most likely ways for a breach of personal data to occur are through a cyber attack of some kind or hacking of a computer, and the physical theft or loss of a computer or data storage device.

Parish Councillors, the Parish Clerk and the PC’s Data Processors all maintain protection from viruses and malware.

The risk of a data breach is considered to be low.

The GDPR requires a Data Controller to notify the ICO about a personal data breach if it is likely to result in " a risk to the rights and freedoms" of an individual. The loss of a list of email addresses or telephone numbers (with no associated information) through a hacking attack would need to be recorded, but would not need to be reported to the ICO.

In the event of a data breach taking place, the personal data lost would comprise names, addresses and telephone numbers, and possibly correspondence. The PC does not hold any personal financial information. A breach would be annoying to those affected, and would cause reputational damage to the PC, but would be very unlikely to result in material harm, financial loss, or a risk to individual rights and freedoms.

A breach of the PC's systems would be an inconvenience, but would not affect the functioning of the Council, and mechanisms are in place to recover essential data.

The effects of a data breach are considered to be small.

5. Recommendations

1. This Report and recommendations should be adopted as an interim measure and reviewed as necessary.
2. This document or the relevant policies should be reviewed annually.
3. The Home Page of the PCs website should include the following privacy statement.

   "If you contact West Harptree Parish Council, the contact details you provide will be retained indefinitely for correspondence purposes. This data will not be used for any other purpose, will not be revealed to anyone else without your consent, and will be deleted on request. Click here for a copy of the Parish Council's General Privacy Policy."
4. The contact / enquiry form functionality of the PCs website should be removed and communication with the PC be limited to emails to and from the Clerk
5. All emails sent from the Clerk should include the statement:

   " This email may contain confidential information and may be privileged. If you are not the intended addressee you may not use, forward, copy or disclose any information contained in this message. If you have received this email in error, please advise the sender immediately and delete this email. "
6. The draft Data Protection Policy in Appendix 1 should be reviewed and adopted and published on the parish council's website.
7. The Retention of Documents and Records Policy in Appendix 2 should be reviewed and adopted.
8. The Clerk should review physical and digital data held, and delete all out of date and redundant material.
9. The appointment of a Data Protection Officer is not required under the GDPR.

Jon Mitchell

January 2019

6. Information sources

- New Data Protection Laws. A GDPR Toolkit for local councils. NALC February 2018.
- Eduserve. Guide to GDPR for Local Government. Webfile.
- ICO Guide. Preparing for the GDPR 12 steps to take now. Webfile.
- ICO. EU GDPR. A Compliance Guide. (Dec 2016).
- Lord Chancellor's Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000.
- LRALC – Data Protection & Freedom of Information Training Course, 31st January 2018.
- NALC Legal Briefing L03-17. Reform of data protection legislation and introduction of the GDPR (May 2017).
- NALC Legal Briefing L04-17. Reform of data protection legislation – General Data Protection Regulation and Data Protection Bill (July 2017).
- NALC Legal Briefing L05-17. GDPR – summary of main provisions (Aug 2017).
- NALC Legal Topic Note L02-18. Reporting Personal Data Breaches.
- NALC Legal Topic note L04-17. Reform of data protection legislation – General Data Protection Regulation and Data Protection Bill (July 2017).
- NALC Legal Topic Note L08-17. Privacy Notices and the legal basis for processing personal data (Nov 2017).
- NALC Legal Topic Notes L09-17. General Data Protection Regulation and subject access requests (Nov 2017).
- NALC Legal Topic Note L10-17. Data Protection Officer (Dec 2017).
- NALC Legal Topic Note 38. Data Protection (Jan 2013).

Appendix 1.

West Harptree Parish Council Data Protection Policy

West Harptree Parish Council recognises its responsibility and is committed to comply with the General Data Protection Regulation 2016 (GDPR). This legislation.

The GDPR regulates how personal information (which may be as little as a name and address and held electronically or on paper) can be collected, handled and used and protects individuals' rights of privacy.

The Parish Council needs to retain certain information to carry out its day-to-day operations, to meet its objectives and to comply with legal obligations. The Parish Council will in the course of carrying out its business have access to personal information such as addresses and telephone numbers and is committed to ensuring any personal data will be dealt with in line with the GDPR.

The aim of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures.

In line with the principles of the GDPR, the Parish Council will ensure that personal data will be

- obtained fairly and lawfully:
- collected only if staff and Councillors have been open and honest about why they want the personal information;
- obtained for a specific and lawful purpose;
- accurate and kept up to date;
- held no longer than necessary;
- subject to appropriate security measures;
- adequate, relevant and not excessive, and held only for the purpose for which it was obtained;
- processed in line with the rights of individuals.

Any unauthorised disclosure of personal data to a third party by an employee or Councillor may result in a disciplinary procedure being started or the matter being referred to the Monitoring Officer. Any unauthorised disclosure by a Contractor may result in the termination of contract.

If a Parish Councillor needs to access information to help carry out their duties, this is acceptable and the Parish Clerk may provide names and addresses. They will only be given as much information as necessary and it should only be used for that specific purpose. Data will not be used for political reasons unless the data subjects have consented.

West Harptree Parish Council Councillors and staff are aware that when complaints or queries are made, they must remain confidential unless the subject gives permission otherwise. When handling personal data, this must also remain confidential.

West Harptree Parish Council will implement the following procedure in the event of a data breach

1. Isolate the affected computer
2. Inform the Clerk, other Councillors and, if necessary, the ICO* immediately
3. Inform affected parties and ask them to change their passwords immediately.
4. Analyse the breach – external help may be required – and report.
5. Debrief at the next PC meeting, and decide on any necessary actions or policy reviews.
6. In the event of loss or theft of a device containing personal data inform the Clerk, other Councillors, the DPO and, if necessary, the ICO* immediately.

- The Data Controller has an obligation to inform the ICO within 72 hours if the personal data breach is likely to result in " a risk to the rights and freedoms" of an individual.

Anyone whose personal information is processed by the Parish Council has the right;

- to know what information is held;
- to know why the information is being held;
- to know who has seen the information;
- to know how to gain access to this information;
- to know how it is kept up to date;
- to know what is being done to comply with the GDPR;
- to access certain personal data being kept about them;
- to prevent processing of their personal information in some circumstances; and
- to correct, rectify or erase personal information that is wrong.

Anyone wishing to know more about personal information held by the Parish Council should contact the Parish Clerk at Clerk@West Harptreepc.co.uk. The Parish Council will aim to comply with requests for access to personal information as soon as possible, but will ensure it is provided within one calendar month of receiving the written request.

This policy will be reviewed at intervals to ensure that it remains up to date and compliant with law.

This policy was adopted by West Harptree Parish Council on 8th January 2019

Appendix 2.

West Harptree Parish Council Documents and Records Retention Policy

Introduction

The Parish Council is required to retain paper and electronic data for a variety of reasons. There is a clear need to retain documentation for audit purposes, staff management, tax liabilities, freedom of information and the eventuality of legal disputes and proceedings. Subject to these reasons for retaining documents, and as a basic starting point, papers and records will be destroyed if they are no longer of use or relevant.

Electoral roll

The current copy of the full electoral roll is held for reference.

Planning papers and documents

Documents are retained by B&NES and are not generally retained by the Parish Council

Insurance policies

The Parish Council will keep a permanent record of insurance company names and policy numbers for all insured risks. The Parish Council will retain insurance policy documents for as long as it is possible to make a claim under them.

Correspondence

If related to audit matters, correspondence will be kept for the period specified in the table below. In planning matters, correspondence will be retained for the same period as for other planning papers. Other correspondence will be retained for as long as it is useful and relevant.

Documentation relating to staff

This will be kept securely and in accordance with the GDPR. After an employment relationship has ended, the Parish Council will retain and access records of former staff for the purpose of giving references, payment of tax, national insurance contributions and pensions, and in respect of any related legal claims made against the council.

Local historical information

The Parish Council may acquire, archive and make available records of local significance in addition to their own administrative records under the Local Government (Records) Act 1962.

Arrangements for the deposit, storage and management of documents

The Parish Council will implement a system of paper and electronic records management to ensure the storage, security of, access to and disposal of both paper and electronic records.

Documents of local and or historical importance, if not retained and stored by the Parish Council, will be offered to the Somerset Archives and Local Studies Service.

Retention of documents

Documents will be retained in accordance with the Document Retention Schedule in Table 2 below, save where and to the extent that the Parish Council needs to retain a document for a longer period by the Limitation Act 1980 (as amended) which provides that legal claims may not be commenced after specified periods set out in table 1.

Table 1: Limitation Act (1980)	
Category	**Limitation Period**
Trust deeds etc	None
Leases	12 years
Recovery of land	12 years
Negligence & other torts	6 years
Rent	6 years
Contract	6 years
Sums recoverable by statute	6 years
Personal injury	3 years
Defamation	1 year
Breach of trust	None

Table 2: Document Retention Schedule		
Document	**Retention period**	**Reason**
Minutes & Reports	Indefinite	Archive
Receipt & payment accounts	Indefinite	Archive
Title deeds, leases	Indefinite	Audit, management
Agreements, contracts	Indefinite	Audit, management
Insurance policies	Indefinite	In case of claims
Insurance certificates - liability for employees	40 years	SI 2753
Salary details, PAYE records	12 years	HMRC audit
Receipt books	8 years	HMRC audit
Clerk expenses book	8 years	HMRC audit
Paid invoices	8 years	HMRC audit
Paid cheques	8 years	HMRC audit
Quotations & tenders	6 years	Management Limitation Act
Bank statements	Last completed audit year	Audit
Bank paying in books	Last completed audit year	Audit
Cheque book stubs	Last completed audit year	Audit

This policy was adopted by West Harptree Parish Council on 14th May 2019