

## The General Data Protection Regulation 2016 (GDPR)

### 1. Outline of the legislation and regulatory framework

The GDPR 2016 will come into force on 25<sup>th</sup> May 2018, and arises from the Data Protection Act 1998. The GDPR requires Carlton Parish Council (the PC) to have a Privacy Notice (also called a Fair Processing 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.

Under the GDPR, the PC and Clerk are Data Controllers; the PC's contractors such as the payroll administrator and website provider are Data Processors; and any person whose data is held is a Data Subject. Personal data is information relating to a living individual who can be recognised from that data.

Under the GDPR, personal data must be:

- (i) processed fairly, lawfully and in a transparent manner in relation to the data subject;
- (ii) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- (iii) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- (iv) accurate and, where necessary, kept up to date;
- (v) 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;
- (vi) 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.

The GDPR defines the PC as a public authority, and requires it to appoint a Data Protection Officer (DPO). The DPO must not be a Data Controller or Processor and must have knowledge of the relevant legislation. This means that in larger councils a member of staff may be able to act as the DPO; in the case of small councils which only employ a Clerk the DPO must be independent of the Council.

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 under 16, consent must be obtained from the parents (this may be reduced to 13 in future legislation).

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

- (i) the identity and the contact details of the data controller and, if any, of the controller's representative and of the data protection officer;
- (ii) the purpose(s) of the processing;

- (iii) the categories of personal data concerned;
- (iv) 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;
- (v) where possible, the envisaged period for which the personal data will be stored or, if not possible, the criteria used to determine that period;
- (vi) 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;
- (vii) 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:

- (i) process the personal data only on the documented instructions of the controller;
- (ii) comply with security obligations equivalent to those imposed on the controller under Article 32 of the GDPR;
- (iii) only employ staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;
- (iv) enlist a sub-processor only with the prior permission of the controller;
- (v) 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);
- (vi) 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. The NALC guidance states that all Data Controllers must maintain a detailed written record: this has been questioned.

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 up to £500,000 for serious breaches; some breaches attract fines of up to 4% of turnover or 20 million Euros, whichever is the higher.

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 PC has a current Publication Scheme, and most PC information is published on the PC's website.

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. The PC publishes more information than is required by this Code.

## **2. Carlton 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 holds photographs of volunteers carrying out project work, publishes these photographs in printed material and on the PC website, and copies these to other organisations. The volunteers involved have all given verbal consent for their pictures to be used in this way, and are not named. 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. The PC maintains lists of members of the Carlton Footpath Group and Gardening Group. The Keep Carlton Tidy Group is a pop-up group of volunteers and does not have a permanent membership.

Personal information may be held in connection with Grants of Exclusive Rights of Burial, Cemetery matters, complaints, contracts and agreements, and notes of private meetings or interviews.

The PC does not use internet banking, and the receipts and payments accounts are kept in manual form and published.

The PC's website is controlled by the Clerk and contains only public information. The flow of information is from the Clerk to the website to the public – there is no traffic from the website back to the Clerk or Council. The website does not use cookies. The website collects user statistics which are 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 Data Processors to handle its banking, payroll and internet functions, and their contract terms are in conformity with the GDPR.

### **3. Carlton 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 currently receives on average one or

two false invoices or phishing emails a week.

**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 Parish Clerk and a volunteer computer expert, and protected by a robust anti-virus and malware system. Data flow is from the Parish Clerk to the website. The website does not allow users to edit or input any information and does not use cookies.

**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**

Carlton 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**

A written general risk assessment is carried out annually in accordance with s3 of the Accounts & Audit Regulations 2015, and measures are already in place to minimise unauthorised access to data, the loss of data and the effect of any loss on the PC's activities (See Report 2018-02).

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 robust 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 Carlton 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. All emails sent from the carltonpc business address by the Clerk or a Parish Councillor 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. “

5. The *Statement of Commitment to GDPR 2018* in Appendix 1 should be reviewed and published on the parish council's website.

6. The draft *Data Protection Policy* in Appendix 2 should be reviewed and adopted.
7. The draft *Procedure in the event of a data breach* in Appendix 3 should be reviewed and adopted.
8. Members of all constituted voluntary groups (currently the Carlton Footpath Group and Carlton Gardening Group) should be invited to complete a *Personal Data Consent Form* as set out in Appendix 4.
9. The *Retention of Documents and Records* Policy in Appendix 5 should be reviewed and adopted.
10. The Clerk should review physical and digital data held, and delete all out of date and redundant material.
11. The *General Privacy Policy* in Appendix 6 should be reviewed and adopted.
12. The NALC template *Privacy Policy for Councillors and staff* should be adopted.
13. Parish Councillors should be provided with email accounts via 1&1 to be used only for parish council business. These accounts would have an address in the form <cooper@carltonpc.co.uk> which would make it clear that they were for PC business.
14. The appointment of a Data Protection Officer (required under the GDPR) should be deferred until information on a local or national scheme has been provided by NALC or LRALC, or until the Annual Meeting in May.

C J Peat (Parish Clerk)  
8<sup>th</sup> March 2018

**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, 31<sup>st</sup> 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. Statement for Parish Council website**

## **Carlton Parish Council Statement of commitment to GDPR 2016**

**Carlton Parish Council is committed to implement and maintain GDPR 2016 compliance**

### **Actions will include**

- ensuring that all Council terms and conditions, interested party agreements, data processor contracts and privacy statements are in line with the General Data Protection Regulation (GDPR);
- ensuring that correct and appropriate contractual terms are in place with data processors which support the principles of GDPR inclusive of all type of data transfers;
- updating Council policies and practices to respond to GDPR requirements and introducing new procedures to align with GDPR 2016;
- monitoring emerging GDPR guidance, and implementing changes where appropriate before and after GDPR comes into force on 25th May 2018;
- continuing to invest in Councillor and Clerk training.

### **Security Standards and Certifications**

The Parish Council places a high priority on protecting the privacy of parishioners and interested parties, and the secure management of data.

The Parish Clerk manages the Parish Council website and data transfer processes for the purposes of maintenance, support and development. Access to the Parish Council website is tightly controlled. Data is stored with 1&1 web hosting and uses Symantec SSL (secure sockets layer) encryption. This complies with the EU-US Privacy Shield framework adopted by the European Commission.

The email accounts of all Parish Councillors and the Clerk are protected by firewalls and anti-virus systems which are kept up to date.

Training is important. All Councillors have an up-to-date working knowledge of the Council's GDPR protocol and procedures and have access to data protection legislation.

This statement will be updated as part of the Parish Council's commitment to transparency, and the protection of Parish Council data.

If you have any specific questions about Parish Council policies or procedures, please contact any Parish Councillor or the Parish Clerk at [Clerk@carltonpc.co.uk](mailto:Clerk@carltonpc.co.uk).

This statement was approved by Carlton Parish Council on 14<sup>th</sup> March 2018

**Appendix 2. Draft Data Protection Policy****Carlton Parish Council****Data Protection Policy DRAFT**

Carlton Parish Council recognises its responsibility to comply with the General Data Protection Regulation 2016 (GDPR). This legislation regulates the use of personal data. This does not have to be sensitive data - it can be as little as a name and address.

**The GDPR**

The GDPR sets out high standards for the handling of personal information and protecting individuals' rights for privacy. It also regulates how personal information can be collected, handled and used. The GDPR applies to anyone holding personal information about people, electronically or on paper.

The Parish Council needs to retain certain information on its employees 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. The Parish Council 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: personal information should only be collected if staff and Councillors have been open and honest about why they want the personal information;
- be obtained for a specific and lawful purpose;
- be accurate and kept up to date;
- not be held longer than necessary;
- be subject to appropriate security measures;
- be adequate, relevant and not excessive, and held only for the purpose for which it was obtained;
- be processed in line with the rights of individuals.

**Storing and accessing data**

Carlton Parish Council recognises its responsibility to be open with people when taking personal details from them. This means that Councillors and staff must be honest about why they want a particular piece of personal information. If, for example, a member of the public gives their phone number to staff or a member of the Parish Council, this will only be used for the purpose it has been given and will not be disclosed to anyone else without the person's permission.

As data controller, the Parish Council will

- ensure personal data is collected in a fair and lawful way;

- ensure that personal information is up to date and accurate – once it is not needed any more, is out of date or has served its use and falls outside the minimum retention time of the Council's document retention policy, personal information will be destroyed or securely deleted;
- ensure that personal information is kept secure;
- ensure the rights people have in relation to their personal data can be exercised;
- ensure that anyone wanting to make enquiries about handling personal information knows what to do;
- not use personal information without the consent of the individual.

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 made by a Contractor may result in the termination of contract.

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

- what information is held;
- why the information is being held;
- who has seen the information;
- how to gain access to this information;
- how to keep it up to date;
- what is being done to comply with the GDPR.

Anyone whose personal information is processed by the Parish Council also has the right to prevent processing of their personal data in some circumstances and the right to correct, rectify or erase information that is wrong. Individuals have a right under the GDPR to access certain personal data being kept about them. Anyone wishing to do so should contact the Parish Clerk.

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 as required by the GDPR. This policy will be reviewed at intervals to ensure that it remains up to date and compliant with the law.

### **Disclosure of personal information**

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 should never be used for political reasons unless the data subjects have consented.

### **Confidentiality**

Carlton Parish Council Councillors and staff must be 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.

This policy was adopted by Carlton Parish Council on 14<sup>th</sup> March 2018

**Appendix 3. Procedure in the event of a data breach**

1. Isolate the affected computer (ie disconnect it from the internet, switch off the router and/or disable the wi fi connection).
2. Inform the Clerk, other Councillors and, if necessary, the ICO\* immediately by telephone or text message.
3. Inform interested parties who may have been affected.
4. Any parties who may have been affected should change their passwords immediately.
5. Analyse the breach – external help may be required – and report.
6. Debrief at the next PC meeting, and decide on any necessary actions or policy reviews.
  
7. 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 by telephone or text message.

\* 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. See NALC L02-18.

Appendix 4. Personal data consent form

**Carlton Parish Council  
Personal Data Consent Form**

**Name** .....

**Address** .....

**Email address** .....

**Telephone number** .....

**Signature** .....

**Date** .....

**Activity or Group** .....

- I hereby consent to Carlton Parish Council holding the personal information listed above in order to contact me regarding relevant events and activities.
- I agree that photographs of me may be taken during voluntary activities and published on the Carlton Parish Council website and in Carlton News, and used in promotional material.

The Data Controller is Carlton Parish Council of 7 Main Street, Carlton, Nuneaton, Warks, CV13 0BZ.

The Data Protection Officer is \*\*\*\*\* - not yet appointed.

This information will be deleted when you cease to be a member of the group(s) listed above, when you advise that you no longer have an interest in the activity listed, or at any time on request.

You have the right to request from the Data Controller rectification or erasure of personal data or to restrict or object to the processing of personal data, and the right to lodge a complaint with the Information Commissioners Office.

**Appendix 5. Retention of Documents & Records**

**Carlton Parish Council**

**Retention of Documents and Records Policy DRAFT**

**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**

- a) Where planning permission is granted, planning documentation will be retained until the development has been completed so that, if required, the council can check that the development is carried out in accordance with the terms and conditions of the permission.
- b) Where planning permission is refused, the planning documentation will be retained until the period within which an appeal can be made has expired. If an appeal is made, and dismissed, the decision notice will be retained against further applications relating to the same site.
- c) Copies of Local Plan documentation and similar material will be retained for as long as they are in force or relevant.

**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.

Insurance certificates against liability for injury or disease to employees arising out of their employment must be kept for 40 years (Reg.4 of Employer's Liability (Compulsory Insurance) Regulations 1998. SI 2753.).

**Correspondence**

If related to audit matters, correspondence will be kept for the period specified in the table in Annex A 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 data protection principles of the Data Protection Act 1998. The principles provide that personal data in relation to staff should not be kept for longer than is necessary for the purpose it was held. However, even 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.

The time limits within which a claim (and any appeal) may be lodged against an employer at an employment tribunal are set out in the legislation that contains the employment right in question or failing that by reference to the Limitation Act 1980 (as amended). The time for lodging a claim at an employment tribunal is usually measured from the date that the employment relationship ended or the date of the act complained of. Subject to where the Limitation Act 1980 applies, the most common time limit for lodging a claim at an employment tribunal is 3 months although 6 months applies in redundancy and equal pay claims.

**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.

**Carlton News**

Copies are retained for reference, and articles of more than passing interest are abstracted and published on the PC website. Copies are deposited with the British Library (Legal Deposit Libraries Act 2003), the Record Office for Leicester, Leicestershire & Rutland, and the Hinckley Library Local Collection.

**Arrangements for the deposit, storage and management of documents**

Documents of local and or historical importance, if not retained and stored by the Parish Council, will be offered first to the Record Office for Leicester, Leicestershire & Rutland.

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.

**Retention of documents for legal purposes**

Most legal proceedings are governed by the Limitation Act 1980 (as amended) which provides that legal claims may not be commenced after a specified period. The specified period varies, depending on the type of claim in question, as set out in the table below.

<b>Category</b>	<b>Limitation period</b>
Trust deeds etc	No limitation period
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

Where the limitation periods tabulated above are longer than other periods specified in this policy, the documentation will be kept for the longer period specified. Some types of legal proceedings may fall within two or more categories, in which case the relevant documentation will be kept for the longest of the limitation periods.

<b>DOCUMENT</b>	<b>MINIMUM RETENTION PERIOD</b>	<b>REASON</b>
Minutes & Reports	Indefinite	Archive
Receipt & payment accounts	Indefinite	Archive
Registers of graves & burials	Indefinite	} Local Authorities
Cemetery plan	Indefinite	} Cemeteries
Disposal certificates	Indefinite	} Order 1977
Grants of Exclusive rights	Indefinite	}
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	Superannuation
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
Scales of fees & charges	6 years	Management
Quotations & tenders	6 years	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 Carlton Parish Council on 14th March 2018

**Appendix 6: Privacy Policy**

**Carlton Parish Council**  
**General Privacy Policy DRAFT 1**

**Personal data**

“Personal data” is any information about a living individual which allows them to be identified from that data (for example a name, photographs, videos, email address, or address). Identification can be by the personal data alone or in conjunction with any other personal data. The processing of personal data is governed by legislation relating to personal data which applies in the United Kingdom including the General Data Protection Regulation (the “GDPR) and other local legislation relating to personal data and rights such as the Human Rights Act.

**Council information**

This Privacy Policy is provided by Carlton Parish Council which is the data controller for your data. The Council’s contact details are at the end of this document.

**What personal data is collected**

Carlton Parish Council may collect personal data in the form of names, addresses, email addresses and telephone numbers.

The Council may take and hold photographs of volunteers carrying out project work.

The Council holds invoices, receipts, contracts, correspondence and cancelled cheques relating to the services provided by the Council.

The Council maintains statutory records.

The Council may communicate with individuals and organisations by telephone, letter or email.

The Council does not collect or process sensitive personal data or other special categories of data such as racial or ethnic origin, mental and physical health, details of injuries, medication/treatment received, political beliefs, trade union affiliation, genetic data, biometric data, data concerning and sex life or sexual orientation.

The Council may hold sensitive personal data where it supports an individual in obtaining services from a third party, or in pursuing a complaint. In these circumstances the sensitive personal information will be provided by the data subject and used only in accordance with their instructions.

The Council may hold personal data where a complaint or claim for damages has been made against the Council.

**The council will comply with data protection law. This says that the personal data we hold about you must be**

- Used lawfully, fairly and in a transparent way;
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes;
- Relevant to the purposes we have told you about and limited only to those purposes;
- Accurate and kept up to date;
- Kept only as long as necessary for the purposes we have told you about;
- Kept and destroyed securely including ensuring that appropriate technical and security measures are in place to protect your personal data to protect personal data from loss, misuse, unauthorised access and disclosure.

**We use your personal data for some or all of the following purposes**

- To deliver public services including to understand your needs to provide the services that you request and to understand what we can do for you and inform you of other relevant services;
- To contact you by post, email, or telephone;
- To prevent and detect fraud and corruption in the use of public funds and where necessary for law enforcement;
- To enable us to meet all legal and statutory obligations and powers including any delegated functions;
- To carry out safeguarding procedures (including due diligence and complaints handling) in accordance with best safeguarding practice from time to time with the aim of ensuring that all children and adults-at-risk are provided with safe environments and generally as necessary to protect individuals from harm or injury;
- To promote the interests of the council;
- To maintain our own accounts and records;
- To seek your views, opinions or comments;
- To notify you of changes to our facilities, services, events and staff, councillors and role holders;
- To process relevant financial transactions including grants and payments for goods and services supplied to the council

**What is the legal basis for processing your personal data?**

The council is a public authority and has certain powers and duties. Most of your personal data is processed for compliance with a legal obligation which includes the discharge of the council's statutory functions and powers. When exercising these powers or duties it is sometimes necessary to process personal data of residents or people using the council's services. We will always take into account your interests and rights. This Privacy Policy sets out your rights and the council's obligations to you in detail.

We may also process personal data if it is necessary for the performance of a contract with you, or to take steps to enter into a contract.

Sometimes the use of your personal data requires your consent. We will first obtain your consent to that use.

### **Sharing your personal data**

The Council will implement appropriate security measures to protect your personal data.

The Council will not share your personal data with anyone without your consent.

If you consent to the publication of a photograph, the image may be published in printed material and on the Parish Council website which may be accessed from anywhere in the world.

### **How long do we keep your personal data?**

In general, we will keep data only for as long as we need it. This means that we will delete it when it is no longer needed.

We will keep some records permanently if we are legally required to do so, or in connection with our statutory obligations as a public authority. We may keep some other records for an extended period of time, for example to support HMRC audits or provide tax information, or in order to defend or pursue claims or legal proceedings.

### **Your rights and your personal data**

When exercising any of the rights listed below, in order to process your request, we may need to verify your identity for your security. In such cases we will need you to respond with proof of your identity before you can exercise these rights.

You have the following rights with respect to your personal data:

- (i) *The right to access personal data we hold on you;*
- (ii) *The right to correct and update the personal data we hold on you;*
- (iii) *The right to have your personal data erased;*
- (iv) *The right to object to processing of your personal data or to restrict it to certain purposes only;*
- (v) *The right to data portability;*
- (vi) *The right to withdraw your consent to the processing at any time for any processing of data to which consent was obtained;*
- (vii) *The right to lodge a complaint with the Information Commissioner's Office.*

You can contact the Information Commissioners Office on 0303 123 1113 or via email <https://ico.org.uk/global/contact-us/email/> or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

### **Transfer of Data Abroad**

Personal data will not be transferred outside the UK without your consent.

**Changes to this policy**

This Privacy Policy will be reviewed from time to time, and updates will be published under Council Information on the Carlton Parish Council website.

**Contact Details**

If you have any questions about this Privacy Policy or the personal data we hold about you, or wish to exercise your rights, please contact C J Peat, Parish Clerk, 7 Main Street, Carlton, Nuneaton, Warks, CV13 0BZ [Tel 01455-290934 or email [clerk@carltonpc.co.uk](mailto:clerk@carltonpc.co.uk) ]

This policy was adopted by Carlton Parish Council on 14<sup>th</sup> March 2018