GDPR POLICY

Knapton Parish Council and your privacy

Knapton Parish Council takes your privacy very seriously and is committed to keeping your personal data safe, secure and up to date, and will not keep it for longer than necessary. The information that you provide us with, or that is gathered automatically, helps us to monitor our services and provide you with the services that you are entitled to as a local parishioner or visitor to our website.

When using your personal data, we are regulated under the **General Data Protection Regulation** (**GDPR**) which applies across the United Kingdom and the European Union.

Purpose of this policy

This policy applies to all personal data collected by, and on behalf of, Knapton Parish Council. It clearly explains our duties and responsibilities with regards to your personal information and GDPR and It identifies the means by which we will meet our obligations to councillors, staff and the public.

Please read it carefully as it contains important information on who we are and how and why we collect, store, use and share your personal data. It also explains your rights in relation to your personal data and how to contact us or supervisory authorities in the event that you have a complaint.

Key Terms

We thought it might be helpful to start by explaining some key terms used throughout this document.

- Who are we?
  Throughout this document, *we*, *us* & *our* all refer to **Knapton Parish Council**
- 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 direct using the data itself or by combining it with other information that Knapton Parish Council possesses, or can reasonably access, which helps to identify a living individual
- Special Category Personal Data
  - this is personal data which reveals racial or ethnic origin, political opinions, religious beliefs, philosophical beliefs or trade union membership
  - genetic and biometric data
  - data concerning health, sex life or sexual orientation
- Data Processing
  Data processing is any activity that involves the use of your personal data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.

- Processing Personal Information
  We do not trade personal data for commercial purposes.
- We will only disclose it if,
  - required by law
  - it is necessary to arrange a service that you have requested
  - it is with your full knowledge and prior consent
- Information you give us
  This is information which you provide to us by filling in forms on our website or by corresponding with us by phone, email, virtual meeting or otherwise. It may be provided by you when,
  - using our website
  - requesting services from us, such as the Knapton Angels
  - registering to receive information and newsletters, such as the Knapton News
  - requesting us to contact you for any reason
  - reporting an issue or problem

This information may include your name, address & postcode, email address and phone number(s)

Your rights and your personal data

GDPR gives rights to every individual with respect to their personal data, with some enhancements to those rights already in place. These rights are,

1) the right to be informed
2) the right of access to the personal data we hold on you.
   a) at any point you can contact us to;
      i) request the personal data that we hold on you
      ii) ask why we have that personal data
      iii) ask who has access to the personal data
      iv) ask where we obtained the personal data from
   b) there are no fees or charges for the first request but additional requests for the same personal data or requests which are manifestly unfounded or excessive may be subject to an administrative fee
3) the right to correct and update the personal data we hold on you
   a) if the data we hold about you is out of date, incomplete or incorrect, you can inform us and your data will be updated
4) the right to have your personal data erased.
   a) if you feel that we should no longer be using your personal data or that we are unlawfully using your personal data, you can request that we erase the personal data we hold
   b) when we receive your request, we will confirm whether the personal data has been deleted or the reason why it cannot be deleted (*for example, because we need it for to comply with a legal obligation*)
5) the right to object to processing of your personal data or to restrict it to certain purposes only.
   a) you have the right to request that we stop processing your personal data or ask us to restrict processing. Upon receiving the request, we will contact you and let you know if we are able to comply or if we have a legal obligation to continue to process your data
6) the right to data portability

a) you have the right to request that we transfer some of your data to another controller. We will comply with your request, where it is feasible to do so, within one month of receiving your request

7) the right to object and withdraw your consent to the processing at any time for any processing of data to which consent was obtained
   a) you can withdraw your consent easily by telephone, email, or by post (see Contact Details below)
8) the right not to be subject to automated decision-making including profiling.

In order to process your request should you choose to exercise any of the rights above, we may need to verify your identity for your security. In such cases we may need you to respond to our request with proof of your identity before you can exercise these rights. Once we have confirmed your identity, we will respond to your request within 30 days.

The two enhancements of GDPR are that

1) individuals now have a right to have their personal data erased (sometime known as the 'right to be forgotten') where their personal data is no longer necessary in relation to the purpose for which it was originally collected
2) data portability must be done free of charge. Data portability refers to the ability to move, copy or transfer data easily between different computers

If a request is received to delete information, then the DPO *(see below)* must respond to this request within a month. The DPO has the delegated authority from the Council to delete information.

If a request is considered to be manifestly unfounded then the request could be refused, or a charge may apply. The charge will be as detailed in the Council's **Freedom of Information Publication Scheme**.

The council will be informed of such requests.

What is the legal basis for processing your personal data?

We process your personal information lawfully and fairly in accordance with data protection laws and we will always take into account your interests and rights. Where the use of your personal data requires your consent, we will first obtain your consent.

- The council is a public authority and as such, has certain powers, obligations and responsibilities. Sometimes when exercising these powers or duties it is necessary to process personal data of residents or people using the council's services.
- Personal data may also be processed for compliance with a legal obligation which could include the discharge of the council's statutory functions and powers.
- We may process personal data if it is necessary for the performance of a contract with you, or to take steps to enter into a contract.

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

- to deliver public services. We may need to understand your personal needs in order to provide the services that you request and to further understand what we can do for you and inform you of other relevant services
- to confirm your identity to provide some services
- to contact you by post, email, telephone or using social media (e.g. Facebook, Twitter, WhatsApp)
- to help us to build up a picture of how we are performing
- to prevent and detect fraud and corruption in the use of public funds and where necessary for the law enforcement functions
- to enable us to meet all legal and statutory obligations and powers including any delegated functions

- to carry out comprehensive 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 other role holders
- to send you communications which you have requested and that may be of interest to you. These may include information about campaigns, appeals, other new projects or initiatives
- to process relevant financial transactions including grants and payments for goods and services supplied to the council
- to allow the statistical analysis of data so we can plan the provision of services.
- our processing may also include the use of CCTV systems for the prevention and prosecution of crime

What personal data does the council process and why?

The council will process some or all of the following personal data where necessary to perform its tasks,

- names, titles and aliases, photographs
- contact details such as telephone numbers, addresses and email addresses
- where they are relevant to the services provided by the council, or where you provide them to us, we may process information such as gender, age, marital status, nationality, education/work history, academic/professional qualifications, hobbies, family composition and dependants
- where you pay for activities, such as use of the Village Hall, financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers

Website Contact Form

When using the Contact Form on our website to contact us, our server forwards your comment to the appropriate person to allow them to deal with your query or issue. Our comment form requests your permission to store any personal information contained in it and we apply your instruction to your personal information.

Email

Emails sent or received by us may be kept as a record of contact and we may also store your email address for future use. If we need to email sensitive or confidential to you, we will check that we are using the correct email address and may use additional security measures, designed to protect your privacy.

When sending us email we recommend using encrypted email.

Do we need your consent to process your sensitive personal data?

In limited circumstances, we may approach you for your written consent to allow us to process certain sensitive personal data. If we do so, we will provide you with full details of the personal data that we would like and the reason we need it, so that you can carefully consider whether you wish to consent.

These types of data are described in the GDPR as **Special categories of data** and require higher levels of protection. We also need to have further justification for collecting, storing and using this type of personal data.

We may process special categories of personal data in the following limited circumstances with your explicit written consent where we need to carry out our legal obligations or where it is in the public interest.

- your racial or ethnic origin or religious or similar information
  in order to monitor compliance with equal opportunities legislation
- your physical or mental health or condition
  in order to monitor sick leave and take decisions on your fitness for work
- in order to comply with legal requirements and obligations to third parties
- in limited circumstances,
- where it is needed in the public interest

Less commonly, we may process this type of personal data where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Sharing your personal data

This section provides information about the third parties with whom the council may share your personal data. These third parties have an obligation to put in place appropriate security measures and will be responsible to you directly for the manner in which they process and protect your personal data. It is likely that we will need to share your data with some or all of the following (but only where necessary):

- the data controllers listed above under the heading "Other data controllers the council works with"
- our agents, suppliers and contractors. For example, we may ask a commercial provider to publish or distribute newsletters on our behalf
- on occasion, other local authorities or not for profit bodies with which we are carrying out joint ventures, for example in relation to facilities or events for the community

Transfer of Data Abroad

Any personal data transferred to countries or territories outside the European Economic Area (EEA) will only be placed on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts approved by the European Union. Our website is also accessible from overseas so on occasion some personal data (for example in a newsletter) may be accessed from overseas.

How is your data processed?

The processing of personal data is governed by legislation relating to personal data which applies in the United Kingdom including the **GDPR** and other legislation relating to personal data and rights such as the **Human Rights Act**.

This says that the personal data we hold about you must be;

- processed 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

This policy updates any previous data protection policy and procedures to include the additional requirements of GDPR which apply in the UK from May 2018. The Government have confirmed that despite the UK leaving the EU, GDPR will still be a legal requirement.

Further processing

If we wish to use your personal data for a new purpose, not covered by this policy, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing.

How long do we keep your personal data?

In general, we will endeavour to keep data only for as long as we need it which means that we will delete it when it is no longer needed. However, we will keep some records permanently if we are legally required to do so and we may keep some other records for an extended period of time.
For example,

- it is currently best practice to keep financial records for a minimum period of 8 years to support HMRC audits or provide tax information
- we may have legal obligations to retain some data in connection with our statutory obligations as a public authority
- the council is permitted to retain data in order to defend or pursue claims. In some cases, the law imposes a time limit for such claims (for example 3 years for personal injury claims or 6 years for contract claims). We will retain some personal data for this purpose as long as we believe it is necessary to be able to defend or pursue a claim

GDPR requires that

…roles and duties must be assigned and that everyone within the council must understand the implications and responsibility of those roles.

- Knapton Parish Council is the Data Controller for the personal data that it holds
- The Parish Clerk is the Data Protection Officer (DPO) for the personal data that the Parish Council
- holds

Appointing the Parish Clerk as the DPO must avoid a conflict of interests, in that the DPO should not determine the purposes or manner of processing personal data.

It is the DPO's responsibility to,

1. undertake an information audit
2. to manage the information collected by the council
3. manage the issuing of privacy policies
4. deal with requests and complaints raised
5. oversee the safe disposal of information

This is to form part of the Job Description of the Parish Clerk.

GDPR requires continued care by everyone within the council, councillors and staff, in the sharing of individual's personal information, whether as a hard copy or electronically.

A breach of the regulations could result in the council facing a fine from the **Information Commissioner's Office** *(ICO)* for the breach itself and also to compensate the individual(s) who could be adversely affected. Therefore, the handling of information is seen as high / medium risk to the council (both financially and reputationally) and one which must be included in the **Risk Management Policy** of the council. Such risk can be minimised by,

- undertaking an information audit
- issuing privacy statements
- maintaining privacy impact assessments (an audit of potential data protection risks with new projects)
- minimising who holds data protected information
- the council undertaking training in data protection awareness.

Data breaches

One of the duties assigned to the DPO is the investigation of any breaches.

Personal data breaches should be reported to the DPO for investigation. The DPO will conduct this with the support of two council members. Investigations must be undertaken within one month of the report of a breach. Procedures are in place to detect, report and investigate a personal data breach. The ICO will be advised of a breach (within 3 days) where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality, or any other significant economic or social disadvantage. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the DPO will also have to notify those concerned directly.

It is unacceptable for non-authorised users to access IT using employees' log-in passwords or to use equipment while logged on. It is unacceptable for employees, volunteers and members to use IT in any way that may cause problems for the Council, for example the discussion of internal council matters on social media sites could result in reputational damage for the Council and to individuals.

Additional Data Controllers

Other data controllers the council may work with may include,

- other local authorities
- community groups
- charities
- other not for profit entities
- contractors

We may need to share the personal data that we hold with them, so that they can carry out their responsibilities to the council. If we and the other data controllers listed above are processing your data jointly for the same purposes, then the council and the other data controllers may be **Joint Data Controllers** which means we are all collectively responsible to you for your data. Where each of the parties listed above are processing your data for their own independent purposes then each of us will be independently responsible to you and if you have any questions, wish to exercise any of your rights (*see page 6*) or wish to raise a complaint, you should do so directly to the relevant data controller.

Being transparent and providing Privacy Notices

accessible information to individuals about how the Council uses personal data is a key element of the Data Protection Act 1998 (DPA) and the EU General Data Protection Regulation (GDPR). The most common way to provide this information is in a **Privacy Notice**. This is a notice to inform individuals about what a council does with their personal information.

A privacy notice will contain the name and contact details of the data controller and Data Protection Officer, the purpose for which the information is to be used and the length of time for its use. It should be written clearly and should advise the individual that they can, at any time, withdraw their agreement for the use of this information. Issuing of a Privacy Notice must be detailed on the Information Audit kept by the council. The council will adopt a Privacy Notice to use, although some changes could be needed

depending on the situation, for example where children are involved. All Privacy Notices must be verifiable.

Information Audit

The DPO must undertake an information audit which details the personal data held, where it came from, the purpose for holding that information and with whom the council will share that information. This will include information held electronically or as a hard copy. Information held could change from year to year with different activities, and so the information audit will be reviewed at least annually or when the council undertakes a new activity. The information audit review should be conducted ahead of the review of this policy and the reviews should be minuted.

If a request is considered to be manifestly unfounded then the request could be refused or a charge may apply. The charge will be as detailed in the Council's Freedom of Information Publication Scheme. The council will be informed of such requests.

Children

There is special protection for the personal data of a child. The age when a child can give their own consent is 13.

If the council requires consent from young people under 13, the council must obtain a parent or guardian's consent in order to process the personal data lawfully. Consent forms for children age 13 plus, must be written in language that they will understand.

Summary

The main actions arising from this policy are:

1. the Council must be registered with the ICO
2. this policy will be considered as a core policy for the Council and a copy will be available on the Council's website.
3. the Parish Clerk's Contract and Job Description (if appointed as DPO) will be amended to include additional responsibilities relating to data protection
4. an information audit will be conducted and reviewed at least annually or when projects and services change
5. Privacy Notices must be issued
6. Data Protection will be included on the Parish Council's Risk Management Policy
7. a committee, with Terms of Reference, will be set up to manage the process

This policy document is written with current information and advice. It will be reviewed at least 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 the Parish Council.

Changes to this notice

We keep this GDPR Policy under regular review

Our Contact Details

Please contact the Knapton Parish Clerk

- if you have any questions about this GDPR Policy

- if you have any questions about the personal information that we hold about you
- if you would like to exercise all relevant rights
- if you have any queries or complaints at:

By Post: Knapton Parish Council, Meadowcroft, Cromer Road, Mundesley, NR11 8DB
Email: parishclerk@knaptonvillage.org

Adopted: September 2026

Review Date: September 2028