

**HOPTON CUM  
KENTTISHALL PARISH  
COUNCIL**

**POLICIES AND  
PROCEDURES**

# **HOPTON CUM KNETTISHALL PARISH COUNCIL GRANT AWARDING POLICY**

Hopton cum Knettishall Parish Council has statutory powers to make funds available to local organisations for the overall benefit of Hopton cum Knettishall and its residents.

This document outlines Hopton cum Knettishall Parish Council's guidelines for awarding. It also formalises the application process to ensure access, openness and fairness to the groups and organisations we aim to support.

## **General information for applicants**

It is Hopton cum Knettishall Parish Council's intention (subject to budget restrictions and available resources) to support initiatives from local community groups and organisations. Priority will be given to applicants who have not previously received grants from Hopton cum Knettishall Parish Council. The size of any grant awarded is at the discretion of the Parish Council, but will not normally exceed £500 in any one application.

## **Who is eligible to apply**

The following organisations may apply to Hopton cum Knettishall Parish Council:

- a. a Hopton cum Knettishall based charity
- b. an organisation serving the needs of the residents of Hopton cum Knettishall
- c. resident(s) of Hopton cum Knettishall requesting grant aid with a project/event, which will be for the benefit of the local community
- d. a Hopton cum Knettishall based club/association/charity serving a specific section of the community or the community as a whole
- e. a local branch of a regional or national organisation/group which serves the needs of the residents of Hopton cum Knettishall.

## **Who is not eligible to apply**

We will normally reject applications from:

- a. projects which are the prime statutory responsibility of other government bodies who would normally be funded by them
- b. a local or regional authority unless it can be clearly demonstrated that the grant would be used specifically for the residents served by Hopton cum Knettishall Parish Council
- c. projects which improve or benefit privately owned land or property
- d. support for individuals or private business projects
- e. applications by "for profit" commercial organisations
- f. from regional and national organisations unless it can be clearly demonstrated that the grant would be used specifically for the residents served by Hopton cum Knettishall Parish Council

- g. from organisations with political affiliations or those established for the purpose of forwarding a party-political agenda
- h. repairs/works to church property or property relating to the affairs of the church or an ecclesiastical charity (Sec 8 Local Government Act 1894)

### **What can be funded**

The project should be something that makes the local community a better place to live, work and play. It should be something that will provide a long lasting and sustainable benefit to our local area. The project must be something that will improve the social, environmental and /or economic profile of Hopton cum Knettishall. Priority will be given to those applications which add value over applications for running costs.

### **The following are unlikely to be considered as a grant priority**

Projects where there is a large shortfall in the funding required to complete the project or projects that simply replace existing facilities with no significant improvement.

### **Conditions of grant**

Hopton cum Knettishall Parish Council support must be acknowledged as appropriate on all publicity and promotional material including posters, advertisements, press releases and leaflets.

Financial support can be only be used for the purpose for which the grant is given.

Grants must not be distributed to any other organisation.

If the organisation can match funding that will be looked upon favourably.

All grants will be subject to terms and conditions.

### **Applications should be submitted in writing to:**

The Parish Clerk

### **Decisions will be based on the following criteria**

- General eligibility
- Impact on key local need
- Community support
- Value for money
- Environmental impact
- Community involvement
- Feasibility
- Likely effectiveness.

# **HOPTON CUM KNETTISHALL PARISH COUNCIL**

## **DATA PROTECTION & INFORMATION MANAGEMENT POLICY**

### **DATA PROTECTION**

#### **1 ABOUT THIS POLICY**

**1.1** This policy outlines the standards Hopton cum Knettishall Parish Council ('the Council') intends to observe in relation to its compliance with the General Data Protection Regulation (GDPR) and subsequently revised UK Data Protection law.

**1.2** The policy is applicable to all councillors and any employees, partners, voluntary groups, third parties and agents authorised by them.

**1.3** The Council shall ensure that all users fully understand its obligations and have undertaken the necessary training to demonstrate compliance with this policy.

**1.4** This policy applies to all personal information created or held by the Council, in whatever format. This includes, but is not limited to paper, electronic, mail, microfiche and film.

#### **2 RESPONSIBILITIES**

**2.1** To operate efficiently, the Council must collect and use information about people with whom it works. This may include members of the public, current, past and prospective employees, customers, contractors, suppliers and partner organisations.

**2.2** The Council regards the lawful and correct treatment of personal information as critical to its successful operations, maintaining confidence between the Council and those with whom it carries out business. The Council will, therefore, ensure that it treats personal information correctly in accordance with the law. The 6 lawful bases for processing data are Consent, Contract, Legal Obligation, Vital Interests, Public Task & Legitimate Interests

**2.3** The Council as a whole is accountable for ensuring compliance with this policy. The day-to-day responsibilities are delegated to the Parish Council Clerk, who will undertake information audits and manage the information collected by the Council including the issuing of privacy notices, dealing with requests and complaints raised and the safe disposal of information.

**2.4** Councillors who process personal data on an individual basis and are not acting on behalf of the council are likely to be considered data controllers and therefore required to notify the Information Commissioner's Office.

**2.5** All councillors and officers who hold or collect personal data are responsible for compliance with data protection legislation and must ensure that personal and/or sensitive information is kept and processed in accordance with this policy.

### **3 BREACH OF THIS POLICY**

**3.1** Breach of this policy may result in disciplinary action in accordance with the Council's Conduct or Capability procedures and, in certain circumstances may be considered to be gross misconduct, resulting in dismissal. It should also be noted that breach of the policy could also lead to criminal or civil action if illegal material is involved or legislation is contravened. Councillors found to be in breach of this policy may also be deemed to have breached the Code of Conduct and referred to the District Council's Monitoring Officer.

### **4 PRIVACY BY DESIGN**

**4.1** The GDPR requires data controllers to put measures in place to minimise personal data processing and that they only process data that is necessary for the purposes of processing and stored for as long as is necessary.

**4.2** The Council will have the appropriate measures in place to determine the basis for lawful processing and will undertake risk assessments to ensure compliance with the law. These measures include the use of Data Protection Impact Assessments (DPIAs), see Appendix 1.

### **5 CONTRACTS**

**5.1** Data protection law places requirements on both the Council and its suppliers to ensure the security of personal data, and to manage individuals' privacy rights. This means that whenever the Council uses a supplier to process individuals' data on its behalf it must have a written contract in place.

**5.2** The law sets out what needs to be included in the contract so that both parties understand their responsibilities and liabilities.

**5.3** The Council is liable for its compliance with data protection law and must only appoint suppliers who can provide 'sufficient guarantees' that the requirements of the law will be met, and the rights of individuals protected.

**5.4** If a contractor, partner organisation or agent of the Council is appointed or engaged to collect, hold, process or deal with personal data on behalf of the council, or if they will do so as part of the services they provide to the Council, the relevant lead Councillor or Council officer must ensure that personal data is managed in accordance with data protection law and this Policy.

**5.5** Security and data protection requirements must be included in any contract that the agent, contractor or partner organisation enters into with the Council and reviewed during the contract's life cycle.

**5.6** Council officers will use the appropriate processes, templates and Data Protection Impact Audits when managing or issuing contracts.

## **6 INFORMATION SHARING**

**6.1** The Council may share information when it is in the best interests of the data subject and when failure to share data may carry risks to vulnerable groups and individuals.

**6.2** Information must always be shared in a secure and appropriate manner and in accordance with the information type. The Council will be transparent and as open as possible about how and with whom data is shared; with what authority; and for what purpose; and with what protections and safeguards.

**6.3** Any Councillor or officer dealing with telephone enquiries must be careful about disclosing personal information held by the Council. In order to manage this the enquirer will be asked to put their request in writing in the first instance.

## **7 INDIVIDUALS' RIGHTS**

**7.1** An individual may request a copy of any data held about them, or information about the reasons for which it is kept and processed. This is called a Subject Access Request (SAR). Information on how an individual can make a SAR can be found in Appendix 3

**7.2** Individuals also have other rights under the Data Protection Act 2018 which are set out in the Council's privacy notices. The Council must respond to individuals exercising their rights within one month.

## **8 DISCLOSURE OF PERSONAL INFORMATION TO THIRD PARTIES**

**8.1** Personal data can only be disclosed about a third party in accordance with the Data Protection Act 2018.

**8.2** If a user believes it is necessary to disclose information about a third party to a person requesting data, they must seek specialist advice before doing so.

## **9 BREACH OF INFORMATION SECURITY**

**9.1** The Council understands the importance of recognising and managing information security incidents. This occurs when data or information is transferred to somebody who is not entitled to receive it. It includes losing data or theft of information, unauthorised use of the Council's system to process or store data by any person or attempted unauthorised access to data or information regardless of whether this was successful or not.

**9.2** All users have an obligation to report actual or potential data protection compliance failures as soon as possible and take immediate steps to minimise the impact and to assist with managing risk. The Council will fully investigate both actual and potential failures and take remedial steps if necessary maintain a register of compliance failures. If the incident involves or impacts personal data it must be reported to the ICO within 72 hours. The Council will follow its Data Breach policy in Appendix 4.

## **10 IT AND COMMUNICATIONS SYSTEMS**

**10.1** The Council's IT and communications systems are intended to promote effective communication and working practices. This policy outlines the standards users must observe when using these systems and the action the Council will take if users breach these standards.

**10.2** Breach of this policy may be dealt with under the Council's Disciplinary Procedure and, in serious cases, may be treated as gross misconduct.

## **11 EQUIPMENT SECURITY AND PASSWORDS**

**11.1** Councillors and officers are responsible for the security of the equipment allocated to or used by them, and must not allow it to be used by anyone other than in accordance with this policy. Passwords must be set on all IT equipment and passwords must remain confidential and be changed regularly.

**11.2** Users must only log onto Council systems using their own username and password. Users must not use another person's username and password or allow anyone else to log on using their username and password.

## **12 SYSTEMS AND DATA SECURITY**

**12.1** Users should not delete, destroy or modify existing systems, programs, information or data (except as authorised in the proper performance of their duties).

**12.2** Users must not download or install software from external sources. Downloading unauthorised software may interfere with the Council's systems and may introduce viruses or other malware.

**12.3** Users must not attach any device or equipment including mobile phones, tablet computers or USB storage devices to our systems.

**12.4** Users should exercise particular caution when opening unsolicited e-mails from unknown sources. If an e-mail looks suspicious do not reply to it, open any attachments or click any links in it.

**12.5** Users must inform the Clerk immediately if they suspect a computer may have a virus.

## **13 E-MAIL**

**13.1** Users should adopt a professional tone and observe appropriate etiquette when communicating with third parties by e-mail.

**13.2** It should be noted that e-mails can be used in legal proceedings and that even deleted e-mails may remain on the system and be capable of being retrieved.

**13.3** Users must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or otherwise inappropriate e-mails.

**13.4** For the purposes of council business, users must use a designated email account (or only use the email account provided) in order to receive or send email correspondence.

## **14 USING THE INTERNET**

**14.1** Users should not access any web page or download any image or other file from the internet which could be regarded as illegal, offensive, in bad taste or immoral. Even web content that is legal in the UK may be in sufficient bad taste to fall within this

prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

## **15 PROHIBITED USE OF COUNCIL SYSTEMS**

**15.1** Misuse or excessive personal use of our telephone or e-mail system or inappropriate internet use will be dealt with under the Council's Disciplinary Procedure. Misuse of the internet can in some cases be a criminal offence.

**15.2** Creating, viewing, accessing, transmitting or downloading any of the following material will usually amount to gross misconduct (this list is not exhaustive):

**(a)** pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);

**(b)** offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or our local community;

**(c)** a false and defamatory statement about any person or organisation;

**(d)** material which is discriminatory, offensive, derogatory or may cause embarrassment to others (including material which breaches the Code of Conduct);

**(e)** confidential information about the Council or any of our staff or our community (except as authorised in the proper performance of your duties);

**(f)** unauthorised software;

**(g)** any other statement which is likely to create any criminal or civil liability; or

**(h)** music or video files or other material in breach of copyright.

## **16 SOCIAL MEDIA**

**16.1** The current Hopton cum Knettishall Parish Council Suffolk Code of Conduct applies to online activity in the same way it does to other written or verbal communication.

## **17 PROHIBITED USE**

**17.1** Users must avoid making any social media communications that could damage the Council's interests or reputation, even indirectly.

**17.2** Users must not use social media to defame or disparage us, Council staff or any third party; to harass, bully or unlawfully discriminate against staff or third parties; to make false or misleading statements; or to impersonate colleagues or third parties.

**17.3** Any misuse of social media should be reported to the Clerk or Chair of the Council.

## **18 GUIDELINES FOR RESPONSIBLE USE OF SOCIAL MEDIA**

**18.1** Users should make it clear in social media postings, or in their personal profile, that they are speaking on their own behalf.

**18.2** Be respectful to others when making any statement on social media and be aware that they are personally responsible for all communications which will be published on the internet for anyone to see.

**18.3** A data protection breach may result in disciplinary action up to and including dismissal.

**18.4** Members or staff may be required to remove any social media content that the Council believes constitutes a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

## **19 BRING YOUR OWN DEVICE (BYOD)**

The Council must take appropriate technical and organisational measures against accidental loss or destruction of or damage to personal data. Councillors using their own devices raises a number of data protection concerns due to the fact that these are owned by the user rather than the data controller. The risks the controller needs to assess are:

- The type of data held.
- Where the data may be stored.
- How the data is transferred.
- Potential data leakage.
- Blurring of personal and business use.
- The device's security capacities.
- What to do if the person who owns the device leaves the Council and
- How to deal with the loss, theft, failure and support of a device.

Councillors and officers using their own devices shall have the following responsibilities:

- Users will not lend their device to anybody.
- Users will inform the Council should they lose, sell, recycle or change their device.

## 20 RECORDS MANAGEMENT

**20.1** It is necessary for the Council to retain a number of data sets as part of managing council business. The Council shall apply the following framework :

DOCUMENT	MINIMUM RETENTION PERIOD	REASON
<input type="checkbox"/> Minute books	Indefinite	Archive
<input type="checkbox"/> Scales of fees and charges	6 years	Management
<input type="checkbox"/> Receipt and payment account(s)	Indefinite	Archive
<input type="checkbox"/> Receipt books of all kinds	6 years	VAT
<input type="checkbox"/> Bank statements, including deposit/savings accounts	Last completed audit year	Audit
<input type="checkbox"/> Bank paying-in books	Last completed audit year	Audit
<input type="checkbox"/> Cheque book stubs	Last completed audit year	Audit
<input type="checkbox"/> Quotations and tenders	6 years	Limitation Act 1980 (as amended)
<input type="checkbox"/> Paid invoices	6 years	VAT
<input type="checkbox"/> Paid cheques	6 years	Limitation Act 1980 (as amended)
<input type="checkbox"/> VAT records	6 years generally but 20 years for VAT on rents	VAT
<input type="checkbox"/> Clerk Expenses	6 years	Tax, VAT, Limitation Act 1980 (as amended)
<input type="checkbox"/> Timesheets	Last completed audit year 3 years	Audit (requirement) Personal injury (best practice)
<input type="checkbox"/> Wages books	12 years	Superannuation
<input type="checkbox"/> Insurance policies	While valid	Management

<input type="checkbox"/> Certificates for Insurance against liability for employees	40 years from date on which insurance commenced or was renewed	The Employers' Liability (Compulsory Insurance) Regulations 1998 (Sl. 2753), Management.
<input type="checkbox"/> Investments	Indefinite	Audit, Management
<input type="checkbox"/> Title deeds, leases, agreements, contracts	Indefinite	Audit, Management
<input type="checkbox"/> Members allowances register	6 years	Tax, Limitation Act 1980 (as amended)

## Appendix 1 – DPIA Assessment Checklist

A. Under the GDPR, data protection impact assessments (DPIAs) are mandatory where the processing poses a high risk to the rights and freedoms of individuals. While they can also be carried out in other situations, councils need to be able to evaluate when a DPIA is required.

B. This checklist helps you make that assessment and provides a springboard for some of the issues you will need to consider in more detail if you do need to carry out a DPIA.

### 1. Do you need to carry out a DPIA?

- (a) What is the objective/intended outcome of the project?
- (b) Is it a significant piece of work affecting how services/operations are currently provided?
- (c) Who is the audience or who will be affected by the project?
- (d) Will the project involve the collection of new personal data about people? e.g. new identifiers or behavioural information relating to individuals
- (e) Will the project involve combining anonymised data sources in a way that may give rise to a risk that individuals could be identified?
- (f) Will the project involve combining datasets originating from different processing operations or data controllers in a way which would exceed the reasonable expectations of the individuals?
- (g) Is data being processed on a large scale?
- (h) Will the project compel individuals to provide personal data about themselves?
- (i) Will personal data about individuals be disclosed to organisations or people who have not previously had routine access to the personal data?
- (j) Will personal data be transferred outside the EEA?
- (k) Is personal data about individuals to be used for a purpose it is not currently used for, or in a way it is not currently used?
- (l) Will personal data about children under 13 or other vulnerable persons be collected or otherwise processed?
- (m) Will new technology be used which might be seen as privacy intrusive? (e.g. tracking, surveillance, observation or monitoring software, capture of image, video or audio or location)
- (n) Is monitoring or tracking or profiling of individuals taking place?
- (o) Is data being used for automated decision making with legal or similar significant effect?
- (p) Is data being used for evaluation or scoring? (e.g. performance at work, economic situation, health, interests or behaviour)
- (q) Is sensitive data being collected including:
  - (i) Race
  - (ii) Ethnic origin
  - (iii) Political opinions
  - (iv) Religious or philosophical beliefs
  - (v) Trade union membership

- (vi) Genetic data
- (vii) Biometric data (e.g. facial recognition, finger print data)
- (viii) Health data
- (ix) Data about sex life or sexual orientation?
- (r) Will the processing itself prevent data subjects from exercising a right or using a service or contract?
- (s) Is the personal data about individuals of a kind likely to raise privacy concerns or is it personal data people would consider to be particularly private or confidential?
- (t) Will the project require contact to be made with individuals in ways they may find intrusive?

## 2. Other issues to consider when carrying out a DPIA

- (a) In addition to considering the above issues in greater detail, when conducting a DPIA, you will also need to look at issues including:
  - (i) The lawful grounds for processing and the capture of consent where appropriate
  - (ii) The purposes the data will be used for, how this will be communicated to the data subjects and the lawful grounds for processing
  - (iii) Who the data will be disclosed to
  - (iv) Where the data will be hosted and its geographical journey (including how data subjects will be kept informed about this)
  - (v) The internal process for risk assessment
  - (vi) Who needs to be consulted (Data Protection Officer, data subjects, the Information Commissioners Office (“ICO”))
  - (vii) Data minimisation (including whether data can be anonymised)
  - (viii) How accuracy of data will be maintained
  - (ix) How long the data will be retained and what the processes are for deletion of data
  - (x) Data storage measures
  - (xi) Data security measures including what is appropriate relative to risk and whether measures such as encryption or pseudonymisation can be used to reduce risk
  - (xii) Opportunities for data subject to exercise their rights
  - (xiii) What staff or, as appropriate, councillor training is being undertaken to help minimise risk
  - (xiv) The technical and organisational measures used to reduce risk (including allowing different levels of access to data and red flagging unusual behaviour or incidents)

3. **The GDPR requires that councils carry out a DPIA when processing is likely to result in a high risk to the rights and freedoms of data subjects. For a council, examples might include using CCTV to monitor public areas.**

4. **If two or more of the following apply, it is likely that you will be required to carry out a DPIA. This does not apply to existing systems but would apply if you introduced a new system.**

1. Profiling is in use. Example: you monitor website clicks or behaviour and record people's interests.
2. Automated-decision making. Example: when processing leads to the potential exclusion of individuals.
3. CCTV surveillance of public areas. Processing used to observe, monitor or control data subjects.
4. Sensitive personal data as well as personal data relating to criminal convictions or offences.
5. Large scale data processing. There is no definition of "large scale". However consider: the number of data subjects concerned, the volume of data and/or the range of different data items being processed.
6. Linked databases - in other words, data aggregation. Example: two datasets merged together, which could "exceed the reasonable expectations of the user" e.g. you merge your mailing list with another council, club or association.
7. Data concerning vulnerable data subjects, especially when power imbalances arise, e.g. staff-employer, where consent may be vague, data of children, mentally ill, asylum seekers, elderly, patients.
8. "New technologies are in use". E.g. use of social media, etc.
9. Data transfers outside of the EEA.
10. "Unavoidable and unexpected processing". For example, processing performed on a public area that people passing by cannot avoid. Example: Wi-Fi tracking.

Appendix 2

**THIS IS A SAMPLE DATA AUDIT QUESTIONNAIRE** and should be used as part of the first step to help you understand what information you hold, why you collect it and what you use it for.

You should go through these questions to help your Council assess if there are any risks in the types of processing that is undertaken. Make sure your Council is aware of the changes that are coming before you undertake this exercise.

There is a glossary at the end of this document to explain further some of the terms referred to.

<b>Part A: YOUR INFORMATION</b>		
1.	<b>1. Person completing questionnaire</b> a) Name. b) Role. c) Telephone number. d) Email.	a) ..... b) ..... c) ..... d) .....
2.	Data controller (e.g. name of local council or parish meeting)	
3.	Date you completed this questionnaire	
<b>Part B: COMMUNICATING PERSONAL DATA</b>		
4.	This section relates to communications with councillors, staff and local residents (including mailing lists) general public. <b>a) What type of personal data does the council keep?</b> e.g. name, contact details such as bank details. <b>b) Where does the council get the personal data from?</b> e.g. staff, residents, other local authorities, charities and sports clubs, community groups, recruitment agencies. <b>c) Why does the council collect or process the data – what does the council do with the personal data?</b> For purposes relating to: e.g. local resident concerns, management of council facilities, services and staff, contract management, performance of statutory functions. <b>d) Who does the council disclose personal data to?</b> E.g. the public, councillors, staff and contractors carrying out the work of the council, pension providers, HMRC, credit reference agencies, recruitment agencies, prospective employers <b>e) Do the council or parish meeting minutes contain personal data?</b> <b>f) Does the council ever send personal data overseas and if so where to and to which organisation? This might include overseas companies providing database or email services.</b> e.g. do any of your suppliers use 'cloud storage' and if so do you know where the personal data is located? <b>g) Does the council collect any sensitive personal data?</b> see definition above. <b>h) If so for what reason?</b> e.g. for safeguarding compliance; physical or mental health data relating to staff; racial and ethnic origin relating to equal opportunities monitoring.	

<b>Part C: SUPPLIERS, COMPANIES, AND OTHER ORGANISATIONS THE COUNCIL CONTRACTS WITH</b>		
5.	<p>About individuals or representatives of organisations which supply us with services such as for council repairs, or with whom we are in contact</p> <p><b>a) Who does the council keep personal data about?</b> e.g. tradesman, recruitment agencies, surveyors, architects, builders, suppliers, advisers, payroll processors.</p> <p><b>b) What type of personal data does the council keep?</b> e.g. name, contact details, qualifications, financial details, details of certificates and diplomas, education and skills.</p> <p><b>c) Where does the council get the data from?</b> e.g. the individuals, suppliers.</p> <p><b>d) Why does the council collect or process the data?</b> e.g. council property maintenance and repairs and management of council facilities, pay and manage staff.</p>	
<b>Part D: GENERAL QUESTIONS ABOUT PERSONAL DATA</b>		
6.	<p>a) How <u>does the council</u> store the personal data collected?</p> <p>b) <u>Does the council</u> take any steps to prevent unauthorised use of or access to personal data or against accidental loss, destruction or damage? If so, what?</p> <p>c) How <u>does the council</u> manage access to data</p> <p>d) What is the process involved in giving access to staff or councillors?</p>	
7.	a) Do any procedures exist for e.g. correcting, deleting, restricting, personal data? If so, please provide details.	
8.	<p>a) Who has access to / is provided with the personal data (internally and externally)?</p> <p>b) Is there an authorisation procedure for accessing personal data? If so, please provide details.</p>	
9.	Does the council provide a copy of all existing privacy notices?	
10.	So far as the council is aware, has any personal data which was gathered for one purpose been used for another purpose (e.g. communicating council news?) If so, please provide details.	
11.	Does the council have any policies, processes or procedures to check the accuracy of personal data?	
12.	<p>a) In the event of a data security breach occurring, does the council have in place processes or procedures to be followed?</p> <p>b) What are these?</p>	
13.	<p>a) If someone asks for a copy of personal data that the council holds about them, i.e. they make a 'subject access request', is there a procedure for handling such a request?</p> <p>b) Is this procedure contained in a written document?</p>	
14.	Does the council have an internal record of the consents which the council has relied upon for processing activities? e.g. to send council newsletters to residents	

15.	<ul style="list-style-type: none"> <li>a) Are cookies used on our council website?</li> <li>b) Does the council provide information about the cookies used and why they are used?</li> <li>c) Does the council keep a record of the consents provided by users to the cookies?</li> <li>d) Does the council allow individuals to refuse to give consent?</li> </ul>	
16.	Does the council have website privacy notices and privacy policies?	
17.	<ul style="list-style-type: none"> <li>a) What data protection training do staff (e.g. council administrator, hall bookings secretary) and councillors receive?</li> <li>b) What does the training involve?</li> </ul>	
18.	<ul style="list-style-type: none"> <li>a) Does anyone in the council have responsibility for reviewing personal data for relevance, accuracy and keeping it up to date?</li> <li>b) If so, how regularly are these activities carried out?</li> </ul>	
19.	<ul style="list-style-type: none"> <li>a) What does the council do about archiving, retention or deletion of personal data?</li> <li>b) How long is personal data kept before being destroyed or archived?</li> <li>c) Who authorises destruction and archiving?</li> </ul>	

**Part E MONITORING**

20.	<ul style="list-style-type: none"> <li>a) Please identify any monitoring of the following systems that takes place. 'Monitoring' includes all monitoring of systems including intercepting, blocking, recording or otherwise accessing systems whether on a full-time or occasional basis. The systems are: <ul style="list-style-type: none"> <li>(i) computer networks and connections</li> <li>(ii) CCTV and access control systems</li> <li>(iii) communications systems (e.g. intercom, public address systems, radios, walkie-talkies)</li> <li>(iv) remote access systems</li> <li>(v) email and instant messaging systems</li> <li>(vi) telephones, voicemail, mobile phone records</li> </ul> </li> <li>b) Does the council have notices, policies or procedures relevant to this monitoring?</li> </ul>	
-----	---	--

**GLOSSARY of terms**

**"Personal Data"** is any information about a living person which can identify them. This is not just someone's name and address but any information which can identify them (directly or indirectly). For example a phone number or email address is personal data. Any other contact information or a person's employment history, or credit history are all personal data.

**"Data controller"** is the person or organisation who determines the how and what of data processing.

**"Data processor"** is the person or firm that processes the data on behalf of the controller.

**"Data subject"** is the person about whom personal data is processed.

**"Processing"** personal data means storing or deleting any personal data

on a computer, database or some manual files (e.g. HR, allotment tenancy files or invoices with contractor payment details). The word 'processing' also covers selecting a name for a mailing list, or reading it off a screen during a call. It includes transferring and altering data. Indeed, practically anything done to personal data constitutes processing. **“Sensitive personal data or special categories of personal data”** are any of the following types of personal data about a data subject: racial or ethnic origin; political opinions; religious beliefs; trade union membership; physical or mental health or condition; sexual life or orientation; genetic data; and biometric data.

## **Appendix 3 SUBJECT ACCESS REQUEST (SAR) POLICY**

### **1. UPON RECEIPT OF A SAR, HOPTON CUM KNETTISHALL PARISH COUNCIL (HPC) WILL:**

- (a) Verify whether HPC is the controller of the data subject's personal data. If it is not a controller, but merely a processor, HPC will inform the data subject and refer them to the actual controller.
- (b) Verify the identity of the data subject; if needed, request any further evidence on the identity of the data subject.
- (c) Verify the access request; is it sufficiently substantiated? Is it clear to the data controller what personal data is requested? If not: request additional information.
- (d) Verify whether requests are unfounded or excessive (in particular because of their repetitive character); if so, HPC may refuse to act on the request or charge a reasonable fee.
- (e) Promptly acknowledge receipt of the SAR and inform the data subject of any costs involved in the processing of the SAR.
- (f) Verify whether HPC processes the data requested. If it does not process any data, inform the data subject accordingly. At all times make sure the internal SAR procedure is followed and progress can be monitored.
- (g) Ensure data will not be changed as a result of the SAR. Routine changes as part of the processing activities concerned are permitted.
- (h) Verify whether the data requested also involves data on other data subjects and make sure this data is filtered before the requested data is supplied to the data subject; if data cannot be filtered, ensure that other data subjects have consented to the supply of their data as part of the SAR.

### **2. RESPONDING TO A SAR**

(a) Hopton cum Knettishall Parish Council will respond to a SAR within one month after receipt of the request:

- (i) If more time is needed to respond to complex requests, an extension of another two months is permissible, provided this is communicated to the data subject in a timely manner within the first month;
- (ii) if the council cannot provide the information requested, it should inform the data subject on this decision without delay and at the latest within one month of receipt of the request.

(b) If a SAR is submitted in electronic form, any personal data should preferably be provided by electronic means as well.

If data on the data subject is processed, make sure to include as a minimum the following information in the SAR response:

- (i) the purposes of the processing;
- (ii) the categories of personal data concerned;
- (iii) the recipients or categories of recipients to whom personal data has been or will be disclosed, in particular in third countries or international organisations, including any appropriate safeguards for transfer of data, such as Binding Corporate Rules or EU model clauses ;
- (iv) where possible, the envisaged period for which personal data will be stored or, if not possible, the criteria used to determine that period;
- (v) the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- (vi) the right to lodge a complaint with the Information Commissioners Office ("ICO");
- (vii) if the data has not been collected from the data subject: the source of such data;
- (viii) the existence of any automated decision-making, including profiling and any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

(d) Hopton cum Knettishall Parish Council will provide a copy of the personal data undergoing processing.

## Appendix 4 **Data Breach Policy**

GDPR defines a personal data breach as “a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”. Examples include:

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction) by a controller or processor
- Sending personal data to an incorrect recipient
- Computing devices containing personal data being lost or stolen
- Alteration of personal data without permission
- Loss of availability of personal data

Hopton cum Knettishall Parish Council takes the security of personal data seriously, computers are password protected and hard copy files are kept in a locked cabinet.

Consequences of a personal data breach -

A breach of personal data may result in a loss of control of personal data, discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of personal data, damage to property or social disadvantage. Therefore a breach, depending on the circumstances of the breach, can have a range of effects on individuals.

Hopton cum Knettishall Parish Council’s duty to report a breach -

If the data breach is likely to result in a risk to the rights and freedoms of the individual, the breach must be reported to the individual and ICO without undue delay and, where feasible, not later than 72 hours after having become aware of the breach. The Data Protection Officer must be informed immediately so they are able to report the breach to the ICO in the 72 hour timeframe.

If the ICO is not informed within 72 hours, Hopton cum Knettishall Parish Council via the Data Protection Officer must give reasons for the delay when they report the breach.

When notifying the ICO of a breach, Hopton cum Knettishall Parish Council must:

- i. Describe the nature of the breach including the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned
- ii. Communicate the name and contact details of the Data Protection Officer
- iii. Describe the likely consequences of the breach
- iv. Describe the measures taken or proposed to be taken to address the personal data breach including, measures to mitigate its possible adverse affects.

When notifying the individual affected by the breach, Hopton cum Knettishall Parish Council must provide the individual with (ii)-(iv) above.

Hopton cum Knettishall Parish Council would not need to communicate with an individual if the following applies:

- It has implemented appropriate technical and organisational measures (i.e. encryption) so those measures have rendered the personal data unintelligible to any person not authorised to access it;
- It has taken subsequent measures to ensure that the high risk to rights and freedoms of individuals is no longer likely to materialise, or
- It would involve a disproportionate effort

However, the ICO must still be informed even if the above measures are in place.

Data processors duty to inform Hopton cum Knettishall Parish Council

If a data processor (i.e. payroll provider) becomes aware of a personal data breach, it must notify Hopton cum Knettishall Parish Council without undue delay. It is then Hopton cum Knettishall Parish Council's responsibility to inform the ICO, it is not the data processors responsibility to notify the ICO.

Records of data breaches -

All data breaches must be recorded whether or not they are reported to individuals. This record will help to identify system failures and should be used as a way to improve the security of personal data.

Record of Data Breaches

Date of breach

Type of breach

Number of individuals affected

Date reported to ICO/individual

Actions to prevent breach recurring

To report a data breach use the ICO online system:

<https://ico.org.uk/for-organisations/report-a-breach/>

# HOPTON CUM KNETTISHALL PARISH COUNCIL

## PRIVACY STATEMENT

**Council Address:** Underwood House, The Street, Rickingham, Diss IP22 1DZ

**Email Address:** [hoptonpc@outlook.com](mailto:hoptonpc@outlook.com)

**Telephone number:** 07813396404

### Contact Privacy Notice

#### When you contact us

The information you provide (personal information such as name, address, email address, phone number, organisation) will be processed and stored to enable us to contact you and respond to your correspondence, provide information and/or access our facilities and services. Your personal information will be not shared or provided to any other third party.

#### The Councils Right to Process Information

General Data Protection Regulations Article 6 (1) (a) (b) and (e)  
Processing is with consent of the data subject or  
Processing is necessary for compliance with a legal obligation or  
Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

#### Information Security

Hopton cum Knettishall Parish Council has a duty to ensure the security of personal data. We make sure that your information is protected from unauthorised access, loss, manipulation, falsification, destruction or unauthorised disclosure. This is done through appropriate technical measures and appropriate policies. Copies of these policies can be requested.

We will only keep your data for the purpose it was collected for and only for as long as is necessary. After which it will be deleted. (You may request the deletion of your data held by Hopton cum Knettishall Parish Council at any time).

## **Children**

We will not process any data relating to a child (under 13) without the express parental/ guardian consent of the child concerned.

## **Access to Information**

You have the right to request access to the information we have on you. You can do this by contacting our Data Information Officer: Nicholas Spring Clerk - [hoptonpc@outlook.com](mailto:hoptonpc@outlook.com) 07813396404

## **Information Correction**

If you believe that the information we have about you is incorrect, you may contact us so that we can update it and keep your data accurate. Please contact: Nicholas Spring Clerk - [hoptonpc@outlook.com](mailto:hoptonpc@outlook.com) 07813396404 to request this.

## **Information Deletion**

If you wish Hopton cum Knettishall Parish Council to delete the information about you please contact: Nicholas Spring Clerk - [hoptonpc@outlook.com](mailto:hoptonpc@outlook.com) 07813396404 to request this.

## **Right to Object**

If you believe that your data is not being processed for the purpose it has been collected for, you may object: Please contact: Nicholas Spring Clerk - [hoptonpc@outlook.com](mailto:hoptonpc@outlook.com) 07813396404 to object.

## **Rights Related to Automated Decision Making and Profiling**

Hopton cum Knettishall Parish Council does not use any form of automated decision making or the profiling of individual personal data.

## **Complaints**

If you have a complaint regarding the way your personal data has been processed you may make a complaint to Hopton cum Knettishall Parish Council Data Information Officer: Nicholas Spring Clerk - [hoptonpc@outlook.com](mailto:hoptonpc@outlook.com) 07813396404 and the Information Commissioners Office casework@ico.org.uk Tel: 0303 123 1113

## **Summary**

In accordance with the law, Hopton cum Knettishall Parish Council only collects a limited amount of information about you that is necessary for correspondence, information and service provision. Hopton cum Knettishall Parish Council does not use profiling, it does not sell or pass your data to third parties. Hopton cum Knettishall Parish Council does not use your data for purposes other than those specified. Hopton cum Knettishall Parish Council makes sure your data is stored securely. Hopton cum Knettishall Parish Council deletes all information deemed to be no longer necessary. Hopton cum Knettishall Parish Council will constantly review its Privacy Policy to keep it up to date in protecting your data.

# **HOPTON CUM KNETTISHALL PARISH COUNCIL DOCUMENT AND ELECTRONIC RETENTION POLICY**

**Reviewed May 2022**

## **INTRODUCTION**

This retention policy applies to Hopton cum Knettishall Parish Council (HPC) and covers all records and documentation, whether analogue or digital.

For the purpose of this policy, the terms 'documents' and 'records' include information in both hard copy and electronic form and have the same meaning whether referred to as documents or documentation.

This policy will also help identify issues with paper records and electronic data storage and will eliminate the need to retain paper and electronic records unnecessarily. HPC will ensure that information is not kept longer than is necessary and will retain the minimum amount of information that it is required to hold to meet its statutory functions and the provision of its services.

Any such system or policies relating to record management will include a review of council documentation on an annual basis.

Anything that is no longer of use or value can be destroyed but if the council is in any doubt it will seek advice from Suffolk Association of Local Councils (SALC) and retain that document until that advice has been received.

Documents of historical importance, if not retained by the council, will be offered first to the Suffolk County Records Office.

## **RETENTION OF DOCUMENTS**

Appendix 1 and 2 indicates the appropriate retention period for audit and other purposes and the reasons for retention.

In respect of the retention of documents in case of a legal dispute, council's policy is set out below. Other documents not specifically mentioned in the Appendix will be treated as follows:

### **Planning Papers**

All Planning Applications are online and accessible on the West Suffolk Council

Copies of structure plans, local plans and similar documents will be retained as long as they are in force.

### **Insurance policies**

Insurance policies and significant correspondence will be kept for as long as it is possible to make a claim under the policy.

Article 4 of the Employer's liability (Compulsory Insurance) regulations 1998 (si 2753) requires that local councils, as employers, retain certificates of insurance against liability for injury or disease to their employees arising out of their employment for a period of 40 years from the date on which the insurance is commenced or renewed.

Circulars and legal topic notes from SALC, NALC and other bodies such as principal authorities will be retained for as long as the information is useful and relevant.

### **Correspondence**

If related to audit matters, correspondence will be kept for the appropriate period specified to the annex thereto.

In planning matters correspondence will be retained for the same period as suggested for other planning papers.

All other correspondence will be kept for as long as the matter is still of interest or use to the council and or the parish.

## Personnel matters

Article 5 of GDPR provides “personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.” This policy will ensure that necessary records, documents and electronic data of HPC are adequately protected, archived and disposed of at the correct retention period, and to provide all staff with clear instructions regarding the appropriate retention and disposal of such documentation.

## RETENTION OF DOCUMENTS FOR LEGAL PURPOSES

Most legal proceedings are governed by 'the limitation acts' which state that legal claims may not be commenced after a specified period. the specified period varies, depending on the type of claim in question. The table below sets out the limitation periods for the different categories of claim.

Claims under category	Limitation period
Negligence (and other torts)	6 years
Defamation	1 year
Contract	6 years
Leases	12 years
Sums recoverable by statute	6 years
Personal injury	3 years
To recover land	12 years
Rent	6 years
Breach of trust	none

If a type of legal proceeding falls into two or more categories, the documentation will be kept for the longer of the limitation period. As there is no limitation period in respect of trust, the council will retain all trust deeds and schemes and other similar documentation whilst still of use to the Parish Council.

## **RETENTION OF ENCRYPTED DATA**

For any information retained under this policy that is in an encrypted format, consideration must be given to the secure storage of any encryption keys. Encryption keys must be retained for as long as the data that the keys decrypt is retained.

## **DISPOSAL OF DOCUMENTS OR DOCUMENTATION**

Disposal can be achieved by a range of processes:

Any paper record containing confidential information must either be disposed of in a confidential waste bin or shredded using a cross-cut shredder.

Disposal of documents that do not contain confidential information may be disposed of in the normal way or recycled.

Computer files are deleted.

Transfer of document to external body - this method of disposal will be relevant where documents or records are of historic interest and/or have intrinsic value. Such a third party could be the county archivist or a local museum.

## **DISPOSAL OF ELECTRICAL HARDWARE**

IT equipment and devices that have the ability and capability to store personal data include: Laptops, Mobile phones, Multi-functional devices – printers / scanners, Servers, USB memory sticks and external hard drives.

IT equipment disposal must be managed by the Chair and Clerk in conjunction with the proper officer.

All computer equipment, recycling or refurbishing must be disposed of in accordance with the Waste Electrical and Electronic Equipment Regulations 2013.

## **DOCUMENTING DISPOSAL**

HPC will keep a record detailing the document disposed of, the date, and the officer who authorised disposal. In particular, the record should be able to demonstrate that the disposal was in accordance with this policy or set out the reasons for departing from it.

Appendix 1 - Retention of documents required for the audit of parish councils

Document	Minimum retention period	Reason
Minutes books	indefinite	archive
Receipt and payment account(s)	indefinite	archive
Receipt books	6 years	VAT
Bank statements	last completed audit year	audit
Bank paying-in books	last completed audit year	audit
Cheque book stubs	last completed audit year	audit
Supplier contracts	6 years	limitation act 1980 (as amended)
Quotations/tenders	12 years	limitation act 1980 (as amended)
Paid invoices	6 years	vat
Paid cheques	6 years	limitation act 1980 (as amended)
VAT records	6 years	vat
Timesheets	last completed audit year	audit
Insurance policies	while valid	management
Certificates for insurance against liability for employees	40 years from date on which insurance commenced or was renewed	the employers' liability (compulsory insurance), regulations 1998 (si 2753), management
Title deeds, leases, agreements, contracts	indefinite	audit, management
Staff attendance records	indefinite	health & safety act 1974
Members allowances registers	6 years	limitation act 1980 (as amended)

Appendix 2 - Retention of documents required relating to information technology

Document	Minimum retention period	Reason
Email	2 years	to satisfy customer complaints
Electronic back up	12 months	to protect records from loss, destruction or falsification
Electronic files	3 years from date last used	to protect records from loss, destruction or falsification
All portable / removable storage media	At end of work cycle / project	data shall be copied or stored on removable media only by authorized users in the performance of official duties
Cryptographic keys – access limited to user / role	Encryption keys retained as long as data that the keys decrypt is retained	see appendix a relating to legislation in place

# **HOPTON CUM KNETTISHALL PARISH COUNCIL**

## **POLICY AND PROCEDURE FOR HANDLING REQUESTS FOR INFORMATION**

Hopton cum Knettishall Parish Council has adopted a Model Publication Scheme with effect from January 2021. This represents the Council's commitment to release information in a recognised format.

A guide detailing the information that is routinely published and how this information can be accessed is available on our website.

1. Verbal requests for information under the Freedom of Information Act 2000 (FOI) will be requested to be put in written form (email will be acceptable) giving the name, correspondence address and details of information required. Information requested under the Environmental Information Regulations Act 2004 (EIR) do not necessarily need to be in writing, although it is the Council's own policy that all such requests should be in written form. Requests for information do not need to refer to FOI or EIR.
2. The Parish Council shall provide proper advice and help to any member of the public seeking information.
3. The Clerk shall agree with the Chairman of the Parish Council whether the requested information is freely accessible, whether it is available in the requested form, whether a Refusal Notice needs to be served in respect of all or part of the requested information and what charges will be levied and the timescale for delivery of the information.
4. The Clerk shall acknowledge a request in writing within three days of receipt of the request and provide a date by which it is anticipated the information will be provided which shall be within 20 working days in normal circumstances. If it is not reasonably possible to provide the information within 20 working days of receipt of the information, the reasons for the delay and a target date shall be provided which must not exceed 40 working days.
5. A fee notice will be issued (if applicable) confirming that the information is held and giving an estimate of the cost of providing the information within a limit of £450. The Council may refuse requests that exceed this limit in which case a refusal notice will be issued (see Policy Reference 6 and 7). Where a fee is to be charged no information will be provided until after the fee has been received, the 20-day period will be extended by up to three months awaiting payment. After the fee has been received, a response will be given within 20 days.
6. If a Refusal Notice is issued in respect of all or part of the requested information it shall state that the Parish Council is relying upon an exemption and why it applies.

Details of the Internal Review procedure shall be enclosed with the Notice and the right of appeal to the Information Commissioner.

7. If a Refusal Notice is issued in respect of all or part of the requested information for any of the following reasons:

- i. The cost of complying with the request will exceed £450
- ii. The Parish Council is unable to identify the information despite every reasonable attempt so to do.
- iii. The Parish Council considers the request to be vexatious (ie to cause harm and/or annoyance rather than to obtain information)
- iv. The information has already been provided or is freely accessible without reference to the Parish Council then details of the right of appeal to the Information Commissioner shall be provided.

8. If the requested information cannot be found within the Parish Council records then the applicant shall be advised, accordingly, as soon as the search is completed. Details of the Internal Review procedure shall be provided and of the right of appeal to the Information Commissioner.

9. Provided the fee is paid and no exemptions apply the Council are obliged to disclose the information.

10. The Parish Council shall maintain a record of FOI requests.

## HOPTON CUM KNETTISHALL PARISH COUNCIL

Information available from Hopton cum Knettishall Parish Council under the model publication scheme

Information to be published	How the information can be obtained
<p><b>Class 1 - who we are and what we do</b></p> <p>Current information only</p> <ul style="list-style-type: none"><li>• Who's who on the Council</li><li>• Contact details for Parish Clerk</li><li>• Contact details (in accordance with GDPR) for Council members</li><li>• Details of accessibility to Parish Council</li></ul>	<p>Available free on website <a href="http://hoptoncumknettishall.onesuffolk.net/parish-council/">http://hoptoncumknettishall.onesuffolk.net/parish-council/</a></p> <p>Available free on noticeboards</p>
<p><b>Class 2 – What we spend and how we spend it</b></p> <ul style="list-style-type: none"><li>• Current and previous financial year's accounts</li><li>• Annual Governance and Accountability Return Form</li><li>• Internal Auditor's Report</li><li>• Finalised Budget</li><li>• Precept Details</li><li>• Financial Regulations &amp; Risk Assessment</li><li>• Grants received</li><li>• Grants given</li><li>• List of contracts awarded and value of contract (if applicable)</li></ul>	<p>Available free on website <a href="http://hoptoncumknettishall.onesuffolk.net/parish-council/">http://hoptoncumknettishall.onesuffolk.net/parish-council/</a></p>

<p><b>Class 3 – What our priorities are and how we are doing</b></p> <ul style="list-style-type: none"> <li>• Annual Report to Parish Meeting</li> </ul>	<p>Available free on website  <a href="http://hoptoncumknettishall.onesuffolk.net/parish-council/">http://hoptoncumknettishall.onesuffolk.net/parish-council/</a></p>
<p><b>Class 4 – How we make decisions</b></p> <ul style="list-style-type: none"> <li>• Timetable of Parish Council Meetings for current year</li> <li>• Agendas of meetings</li> <li>• Minutes of meetings (this will exclude information that is properly regarded as private to the meeting)</li> <li>• Responses to consultation papers</li> <li>• Responses to planning application</li> </ul>	<p>Available free on website  <a href="http://hoptoncumknettishall.onesuffolk.net/parish-council/">http://hoptoncumknettishall.onesuffolk.net/parish-council/</a></p> <p>On request to the Parish Clerk  Included within the minutes or available on the Local Planning Authority's website <a href="https://planning.westsuffolk.gov.uk/online-applications/">https://planning.westsuffolk.gov.uk/online-applications/</a></p>
<p><b>Class 5 – Our policies and procedures</b></p> <ul style="list-style-type: none"> <li>• Standing Orders</li> <li>• Code of Conduct</li> <li>• Grant Awarding</li> <li>• Data Protection</li> <li>• Freedom of Information</li> <li>• Complaints</li> <li>• Health &amp; Safety</li> <li>• Recruitment</li> <li>• Employees Code of Conduct and Grievance</li> <li>• Disciplinary Procedure</li> </ul>	<p>Available free on website  <a href="http://hoptoncumknettishall.onesuffolk.net/parish-council/">http://hoptoncumknettishall.onesuffolk.net/parish-council/</a></p>

<p><b>Class 6 – Lists and Registers</b></p> <ul style="list-style-type: none"> <li>• Assets Register</li> <li>• Register of Members’ Interests</li> <li>• Disclosure Log (indicating the information which has been provided in response to requests)</li> </ul>	<p>Available free on website  <a href="http://hoptoncumknettishall.onesuffolk.net/parish-council/">http://hoptoncumknettishall.onesuffolk.net/parish-council/</a></p>
<p><b>Class 7 – The services we offer</b></p> <ul style="list-style-type: none"> <li>• Upkeep of cemetery</li> <li>• Insurance of village assets</li> <li>• Publicity</li> <li>• Maintenance of website and Facebook</li> <li>• Grant funding to support village clubs and groups</li> </ul>	<p>Available on website or on request to the Parish Clerk</p>

**SCHEDULE OF CHARGES – where applicable**

This describes how the charges have been arrived at and is published as part of the guide.

TYPE OF CHARGE	DESCRIPTION	BASIS OF CHARGE – cost of stationery & admin time
Disbursement cost	Printing @ £1 first sheet then 10p per sheet (black & white) or 15p per sheet (colour)	Actual cost
	Postage	Actual cost of Royal Mail standard 2nd class
Statutory Fee		In accordance with the relevant legislation

# HOPTON CUM KNETTISHALL PARISH COUNCIL

## COMPLAINTS PROCEDURE

Hopton cum Knettishall Parish Council strives to provide a high standard of service to the public. In the interests of openness and the desire to seek continuous improvement, the Council encourages anyone who feels dissatisfied with the service provided to bring this to the attention of the Council.

In some instances, it will be appropriate for an explanation to be given and/or remedial action taken.

Where a formal complaint is submitted in writing, a proportionate investigation will be conducted and the outcome communicated back to the complainant in writing.

### **How to make a complaint about the Council**

Enquiries or observations about the Council can be made by e-mail to [hoptonpc@outlook.com](mailto:hoptonpc@outlook.com)

Formal complaints must be submitted in writing to the Clerk at Hopton cum Knettishall Parish Council, Underwood House, The Street, Rickinghall, Diss IP22 1DZ or by e-mail to [hoptonpc@outlook.com](mailto:hoptonpc@outlook.com)

If the matter relates directly to the Clerk, the complaint should be addressed to the Chairman of the Council.

### **Confidentiality**

All complaints will be treated as confidential. Even where the complainant specifically waives their right to confidentiality, the Council will comply with its obligations under the Data Protection Act 2018 to safeguard against the unlawful disclosure of personal data.

Any meeting of the Council, or a committee or sub-committee considering a complaint or inviting the complainant to make representations will exclude the public. Agendas and minutes will not disclose personal data or financial, sensitive or confidential information relating to an individual complainant or a third party.

## **Acknowledgment of a formal complaint**

Receipt of the complaint will be acknowledged within 7 working days.

A response will be sent within 30 working days specifying:

- who is dealing with the complaint
- whether the complainant will have an opportunity to make verbal representations, accompanied by a friend if desired
- the timeframe for receipt of a formal response

## **Investigation**

It will usually be appropriate for the circumstances leading to the complaint to be investigated by the Clerk on behalf of the Council. Complaints of a serious nature or any that relate directly to the Clerk will be dealt with by the Council (or sub-committee).

Where appropriate, the complainant will be invited to make verbal representations to the person (or sub-committee) investigating.

In normal circumstances, the complainant will be notified in writing (e-mail if appropriate) of the outcome within three months of lodging the complaint. This will include whether or not the complaint is upheld, reasons for the decision, details of any action taken and information about the right of appeal.

## **Appeals**

If the complainant is not satisfied with how a complaint has been dealt with, they can appeal in writing to the Council, setting out what they are unhappy with and the grounds.

The appeal will be considered by a sub-committee formed of persons not previously involved in the investigation of the original complaint. This will consist of a review of the original investigation and outcome, together with any action taken as a result.

Appeals received more than one month after the date of the decision letter/e-mail will not be considered.

## **Complaints involving members of staff or councillors, etc.**

Where a complaint against the Council includes reference to the actions or conduct of staff or councillors, the complaint will be treated as a complaint against the body corporate, as opposed to the individual(s). If after the complaint has been considered the Council considers there may be a need to take disciplinary action against a member of staff, this will be dealt with in accordance with its disciplinary procedure.

Allegations that a member has breached the Code of Conduct should be forwarded to the Monitoring Officer of West Suffolk Council in writing.

[https://www.westsuffolk.gov.uk/Council/Councillors\\_and\\_meetings/councillorsconduct.cfm](https://www.westsuffolk.gov.uk/Council/Councillors_and_meetings/councillorsconduct.cfm)

Councillors are free to raise matters of concern in respect of council business by the submission of motions on the agenda of the relevant meeting(s).

Where a member of staff has a complaint about the workplace, these should be raised in accordance with the Council's grievance procedure.

**Local Government Ombudsman** <https://www.lgo.org.uk/>

The Local Government Ombudsman deals with complaints against principal authorities (district, borough and county councils) and certain other public sector bodies.

It is not responsible for handling complaints against a town or parish council, except where it is working with a principal authority (through a joint committee), or it is exercising the functions of a principal authority.

### **Unreasonable, unreasonably persistent or vexatious complainant behaviour**

Where the Council considers a complainant acts unreasonably or in a vexatious manner, or unreasonably persists with their complaint, the Council will act robustly to maintain the proportionate and balanced use of resources in the interests of the community as a whole, or to protect its staff (or those of its contractors) from unreasonable or distressing behaviour. In seeking to achieve this, the Council will consider all options available to it which may include providing the complainant with acknowledgements only of letters or emails; or, ultimately, it may inform the complainant that future correspondence will be placed on file, but not acknowledged. The Council reserves the right, exceptionally, to terminate communications immediately with a complainant. The complainant will be informed in writing of the decision that has been taken, the reason and the period during which any restriction will apply.