

# North Hinksey Parish Council Privacy Policy

## 1. Introduction

The General Data Protection Regulation (GDPR), which in May 2018 replaced the Data Protection Act 1998, requires organisations such as Parish Councils which act as data controllers and data processors to provide evidence of how they comply with the legislation. The purpose of this Privacy Policy is both to provide that evidence, and to enable all Councillors, Employees and other Role Holders acting on behalf of North Hinksey Parish Council (NHPC) to be aware of the requirements of the GDPR and the procedures put into place by NHPC that enable compliance.

Where responsibilities are assigned to the NHPC Chairman or Chairman of one of the NHPC Committees, in their prolonged absence these responsibilities will be temporarily reassigned to the relevant Vice-Chairman. In the prolonged absence of the Parish Clerk their responsibilities shall be temporarily reassigned to the NHPC Chairman.

This Policy should be read in conjunction with the following documents:

- The NHPC Privacy Notice for the General Public.
- The NHPC Privacy Notice for Councillors, Employees and other Role Holders.

## 2. Personal data – what is it?

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

## 3. Council information

This Privacy Policy is provided by North Hinksey Parish Council, which acts as the overall data controller for data identified in this Policy. Individuals (either Councillors or Employees) acting as data controllers for specific data sets are identified in Appendix 1 of this Policy.

The Council’s postal address is 3 Church Way, Botley, Oxford, OX2 9TH.

## 4. The council works together with other organisations including some or all of the following:

NHPC does not normally share personal data from the general public with third parties, and if the necessity arose to do so at any time in order to enable them to carry out their responsibilities to the council, the data providers would be advised in advance, and where appropriate consent gained from them to do so. Other third party data controllers could include bodies such as local authorities, community groups, contractors or credit reference agencies.

Personal data from Councillors and Employees is shared with third parties where required to meet legal obligations, including the following bodies:

- Other data controllers, such as local authorities (e.g. Vale of White Horse District Council and Oxfordshire County Council), public authorities, central government and agencies such as HMRC and DVLA
- Staff pension providers
- Former and prospective employers
- DBS services suppliers
- Payroll services providers
- Recruitment Agencies
- Credit reference agencies

If we and the other data controllers are processing your data jointly for the same purposes, then the council and the other data controllers may be “joint data controllers” which mean we are all collectively responsible for the data. Where each of the parties are processing the data for their own independent purposes then each of us will be independently responsible to the data provider and if they have any questions, wish to exercise any of their rights or wish to raise a complaint, they should do so directly to the relevant data controller.

## **5. What personal data is collected?**

NHPC carried out a full data audit during April 2018, and following a rigorous data cleanse operation the only data sets remaining under our control that contain personal data are summarised in Appendix 1 of this Policy. The following list contains personal data items that may be necessary for NHPC to hold in the foreseeable future, although not all are currently required:

- Names, titles, and aliases, photographs;
- Contact details such as telephone numbers, addresses, and email addresses;
- Where they are relevant to the services provided by a council we may process demographic information such as gender, age, marital status, nationality, education/work histories, academic/professional qualifications, hobbies, family composition, and dependants;
- Where the data provider pays for activities such as rental of an allotment plot, financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers;
- Start date / leaving date.
- Employment details, financial interests, and land / property ownership data etc. as required for the registration of Councillors’ interests.
- Where they are relevant to our legal obligations, or where you provide them to us, we may process information such as gender, age, date of birth, marital status, nationality, education/work history, academic/professional qualifications, employment details, hobbies, family composition, and dependants.
- Non-financial identifiers such as passport numbers, driving licence numbers, vehicle registration numbers, taxpayer identification numbers, staff identification numbers, tax reference codes, and national insurance numbers.
- Financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers.

- Financial information such as National Insurance number, pay and pay records, tax code, tax and benefits contributions, expenses claimed.
- Other operational personal data created, obtained, or otherwise processed in the course of carrying out our activities, including but not limited to, CCTV footage, recordings of telephone conversations, IP addresses and website visit histories, logs of visitors, and logs of accidents, injuries and insurance claims.
- Next of kin and emergency contact information
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process and referral source (e.g. agency, staff referral))
- Location of employment or workplace.
- Other staff data (not covered above) including; level, performance management information, languages and proficiency; licences/certificates, immigration status; employment status; information for disciplinary and grievance proceedings; and personal biographies.
- CCTV footage and other information obtained through electronic means such as swipecard records.
- Information about your use of our information and communications systems.
- The data we process does not currently include sensitive personal data or other special categories of data such as racial or ethnic origin, mental and physical health, details of injuries, medication/treatment received, political beliefs, trade union affiliation, genetic data, biometric data, data concerning and sex life or sexual orientation. If such data is processed at a future date then this Policy will be amended to reflect that, and to contain additional information required under the GDPR.

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

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

**7. We use personal data for some or all of the following purposes:**

- To deliver public services including to understand needs to provide requested services and to understand what we can do for parishioners and inform them of other relevant services;
- To confirm identity to provide some services;
- To contact parishioners by post, email, telephone or using social media (e.g., Facebook);

- 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 views, opinions or comments;
- To notify parishioners of changes to our facilities, services, events and staff, councillors and role holders;
- To send communications to parishioners that may be of interest to them. 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;
- As a means of communicating with Councillors, Employees and other Role Holders;
- Making a decision about recruitment or appointment;
- Determining the terms on which Employees work for us;
- Checking that Employees are legally entitled to work in the UK;
- Paying employees, and deducting tax and National Insurance contributions;
- Providing contractual benefits;
- Liaising with pension providers;
- Administering the contract we have entered into with Employees;
- Management and planning, including accounting and auditing.
- Conducting performance reviews, managing performance and determining performance requirements;
- Making decisions about salary reviews and compensation;
- Assessing qualifications for a particular job or task, including decisions about promotions;
- Conducting grievance or disciplinary proceedings;
- Making decisions about continued employment or engagement;
- Making arrangements for the termination of working relationships with Employees;
- Education, training and development requirements;
- Dealing with legal disputes, including accidents at work;

- Ascertaining fitness to work for Employees;
- Managing sickness absence;
- Complying with health and safety obligations;
- To prevent fraud;
- To monitor use of our information and communication systems to ensure compliance with our IT policies;
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution;
- To conduct data analytics studies to review and better understand employee retention and attrition rates;
- Equal opportunities monitoring;
- To undertake activity consistent with our statutory functions and powers including any delegated functions;
- To maintain our own accounts and records;
- To process a job application;
- To administer councillors' interests,
- To provide a reference.

## **8. What is the legal basis used by NHPC for processing personal data?**

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

We may also process personal data if it is necessary for the performance of a contract, or as a public task for the carrying out of official functions. An example of this would be processing data in connection with the acceptance of an allotment plot tenancy

Sometimes the use of personal data requires consent. In those circumstances we will obtain consent in writing prior to obtaining or processing that data. Appendix 2 contains consent form CF1, which is used to obtain consent from members of the general public to (a) have their contact details retained in a data set and used to communicate with them, and/or (b) retain photographs and other personal data for NHPC publicity purposes.

We will also process personal data in order to assist Councillors, Employees and other Role Holders in fulfilling their role in the council including administrative support or if processing is necessary for compliance with a legal obligation. Councillors details are obtained by means of form CF2, which is shown in Appendix 3. This form requests information required for public task purposes, but also doubles as a consent form enabling Councillors to identify exactly which of their contact details is used in various types of public communication channels.

Where consent forms are required for other new specific purposes these must follow GDPR guidelines and also be approved at a full Council meeting before being adopted for use.

Additionally a new data set log sheet for the NHPC IRPA (see Section 15) will need to be completed for the data set that they are being used to provide information for.

In Appendix 1 of this NHPC Privacy Policy the data sets held by NHPC are listed, and the lawful basis for holding each of them is clearly identified. This lawful basis is also stated on any form or other means used to gain the data initially together with a reference to the appropriate Privacy Policy.

## **9. Sharing your personal data**

Personal data will only be shared with third parties including other data controllers where it is necessary for the performance of the data controllers' tasks or where the data subject gives us their prior consent. The council will implement appropriate security measures to protect personal data. This section of the Privacy Policy includes information about the third parties with whom the council may share personal data. These third parties also have an obligation to put in place appropriate security measures and will be responsible to the data subject directly for the manner in which they process and protect their personal data.

It is likely that we will need to share some data with:

- Our agents, suppliers and contractors. For example, we may ask a commercial provider to manage our HR/ payroll functions, or to maintain our database software;
- Other persons or organisations operating within local community.
- Other data controllers, such as local authorities (e.g. Vale of White Horse District Council, Oxfordshire County Council), public authorities, central government and agencies such as HMRC and DVLA
- Staff pension providers
- Former and prospective employers
- DBS services suppliers
- Payroll services providers
- Recruitment Agencies
- Credit reference agencies
- Professional advisors
- Trade unions or employee representatives

Internally, personal data is only shared by the individual data controllers with Councillors, Employees and other Role Holders where necessary to carry out the purposes for which it was originally obtained.

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

We will keep some records permanently if we are legally required to do so. 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. In general, we will endeavour to keep data only for as long as we need it. This means that we will delete it when it is no longer needed.

This Privacy Policy shows the period for which data is normally held by NHPC, by each individual data set, in Appendix 1.

Where a request is received by the data subject to adjust, add or delete personal data (see also Section 11: Rights of the data subject) that is implemented within 1 calendar month where possible. If this is not possible for some reason (e.g. the need to retain data in order to fulfil legal obligations) then the data subject will be informed of this within 1 calendar month, and the implementation will occur within 1 calendar month of it becoming possible.

## **11. Rights of the data subject**

Data subjects have the following rights with respect to their personal data:

When exercising any of the rights listed below, in order to process your request, we may need to verify the identity of the data subject for security reasons. In such cases we will need the data subject to respond with proof of your identity before they can exercise these rights. See Section 20: Contact details for further information about how data subjects can exercise the rights listed below.

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

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

Further details about the above rights can be found in the NHPC Privacy Notices.

## **12. 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.

### **13. Data Breaches**

A personal data breach is one that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Some examples of a breach of data include:

- E-mails being sent to the wrong people.
- E-mails to a number of third party individuals not being sent as blind copies.
- Lost memory sticks containing unencrypted personal data.
- Insufficient protection against computer viruses leading to hacking and data being accessed, amended or destroyed,
- Incorrect signage on CCTV.
- Lost or damaged paperwork forms.

Data controllers and others with whom personal data has lawfully been shared must take appropriate precautions to avoid data breaches (see section 14. Data Security below), however should a data breach occur the following procedure must be followed:

#### **Data Breach Procedure:**

- (i) The following individuals should be contacted in the stated order, immediately on discovery of an apparent data breach: the relevant individual data controller, the Parish Clerk, the NHPC Chairman, the NHPC Vice-Chairman. Initially contact should be attempted via telephone, however if contact is not achievable in that manner then an e-mail should be sent including the phrase "URGENT DATA BREACH" in the subject line. All known details of the data breach should be passed on to these individuals.
- (ii) A report should then be drawn up within 24 hours and sent to the individuals listed in (i) above stating the recommended action to be taken to deal with the data breach. The individual responsible for drawing up the report would normally be the individual data controller, or in their absence the Parish Clerk. In the absence of both those individuals, responsibility would transfer to the NHPC Chairman or then the NHPC Vice-Chairman.
- (iii) As many of the individuals listed in (i) above as are available would then need to agree a plan of action to deal with the data breach, preferably by meeting in person, or if that is not possible by e-mail. Where possible this should occur within 48 hours of the data breach being identified.
- (iv) The plan of action should then be implemented at the earliest opportunity, and where required a report including details of the data breach and the plan of action sent to the Information Commissioner's Office within 72 hours of the data breach being identified. The individual(s) responsible for carrying out these actions should be clearly identified in the plan of action (see (iii) above).
- (v) Follow up actions should continue until the matter has been resolved to the satisfaction of both NHPC and the ICO (where required), and additionally the matter should also be reported to all NHPC Councillors and other relevant individuals for discussion at the next full Council meeting.
- (vi) Where necessary this Privacy Policy should be amended in light of the findings of the above process to avoid repetition of the incident.



## **14. Data Security**

Data storage:

- Electronic databases are kept on secure, password protected computers by the relevant data holders.
- Original paperwork forms (e.g. consent forms, allotment annual rent demands, grant application forms etc.) are kept in locked cupboards or safes, either in the NHPC office or at individual data controllers' homes.

Data use:

- On any e-mails to external groups of individuals using e-mails from a data set held by NHPC the e-mail addresses are entered into the bcc address bar so that they cannot be seen by other recipients of the message.
- E-mail addresses held by NHPC are not stored in system address books but copied and pasted into e-mails directly from the contact database to reduce the danger of e-mail hacking.
- It is the joint responsibility of the Webmaster and the Parish Clerk to ensure that prior consent has been obtained for any personal data placed on the NHPC website or Social Media pages using forms CF1, CF2 or any other appropriate consent form approved by full Council.
- It is the joint responsibility of the Communications Committee Chairman and the Parish Clerk to ensure that prior consent has been obtained for any personal data placed in NHPC Newsletters or any other printed publication using forms CF1, CF2 or any other appropriate consent form approved by full Council.

Further details about the various ways that data is held (e.g. paper forms, electronic file) for specific data sets, and the data security in place can be found in the NHPC Internal Register of Processing Activities – see Section 15 below.

## **15. NHPC Internal Register of Processing Activities (IRPA)**

The NHPC IRPA consists of a series of individual data set log sheets for each individual data set held by NHPC. These individual sheets are produced and maintained fully up to date by the relevant individual data controller, and a copy of all of them also maintained in a central file as the official NHPC IRPA by the Parish Clerk, which is to be made available on request to any Councillor.

The data set log sheets will include details of all processing of a data set (whether carried out by the identified data controller or a separate data processor acting on behalf of the data controller) from initially obtaining the data through to its final deletion.

## **16. PIAs / DPIAs**

Currently it has been identified that there is no requirement for NHPC to carry out a Privacy Impact Assessment (PIA) or a Data Protection Impact Assessment (DPIA), however should the need arise subsequently to do so (for example through the deployment of new technology) then this Policy will be adjusted to reflect that change, and the appropriate assessment undertaken.

## **17. Data Protection Officer**

As a Parish Council the NHPC is currently exempt from the need to designate a Data Protection Officer under the GDPR, and therefore has not done so. Responsibility for complying with the GDPR lies with the Councillors jointly as the elected officials of NHPC, however in practice the maintenance of an appropriate Privacy Policy, Privacy Notices and adequate procedures to enable

compliance with GDPR will fall primarily to the identified individual data controllers and the Chairman and Vice-Chairman of NHPC.

## **18. Further processing**

If we wish to use personal data for a new purpose, not covered by this Privacy Policy and the NHPC Privacy Notices, then we will provide revised versions of those documents 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 prior consent to the new processing.

## **19. Changes to this policy**

We keep this Privacy Policy under regular review and we will place any updates on this web page -

<https://northhinksey-pc.gov.uk/about/policies-code-of-conduct/>

This Policy was last updated in September 2020.

## **20. Contact Details**

Please contact us if you have any questions about this Privacy Policy or the personal data we hold about you or to exercise all relevant rights, queries or complaints at:

Sharon Henley, Parish Clerk, North Hinksey Parish Council, 3 Church Way, Botley, Oxford OX2 9TH.

E-mail: [clerk@northhinksey-pc.gov.uk](mailto:clerk@northhinksey-pc.gov.uk)

Telephone number: 07494 054581

Where necessary the Parish Clerk will pass on these requests to the relevant individual data controller to deal directly with them.

Enquiries of this type will be answered within 1 calendar month and there will be no charge for an initial enquiry. NHPC reserves the right to refuse or charge a 'reasonable fee' for requests that are manifestly unfounded, excessive or repetitive. Where requests are refused the individual has the right to complain to the ICO (see Section 11: Rights of the data subject) or to go to court.

Appendix 4 contains a detailed checklist for NHPC data controllers dealing with Subject Access Requests (SARs).

**Appendix 1:** Summary table of data sets held by NHPC

<b>Data Description</b>	<b>Councillors' details:</b> Name, postal address, e-mail, telephone numbers, photograph.	<b>Councillors' Interests:</b> Employment, financial, land / property ownership details etc.	<b>Employee details:</b> Name, contact details, NI number, Tax code, salary details, pension details etc.	<b>Job applicant details:</b> Name, contact details, work experience, education, qualifications etc.
<b>Data Subject</b>	NHPC Councillors.	NHPC Councillors.	NHPC Employees.	Applicants for NHPC Employee roles.
<b>Purpose and Legal Basis for holding</b>	Internal communications and access for Parishioners / general public. Public task.	Required for registration of Councillors' Interests. Legal obligation.	To allow contact by Parish Clerk and Councillors, and to carry out duties as an employer. Legal obligation.	To ascertain suitability for the job. Public task.
<b>Data Controller / (Data Processor)</b>	Parish Clerk.	VOWHDC / (Parish Clerk).	HMRC and Oxfordshire County Council / (Parish Clerk)	Parish Clerk (or for applicants for the Parish Clerk role, NHPC Chairman).
<b>Means of obtaining data</b>	Form CF2.	Registration form provided by VOWHDC.	Appointment letter and form.	Job application form.
<b>Data shared with</b>	All data shared internally. Selected items shared with the general public.	Original form retained by VOWHDC, but data shared electronically with the general public via VOWHDC and NHPC websites.	HMRC and Oxfordshire County Council.	Other interviewers.
<b>Length of time data is held</b>	Original data up to 6 months after standing down as an NHPC Councillor. On request for deletion, from 1 month after standing down as a Councillor.	Deleted from NHPC website within 1 month of standing down as an NHPC Councillor. Original forms and VOWHDC website managed by VOWHDC – see their procedures.	Minimum of 3 years after the end of the financial year in question, and up to 5 years after.	Data held by interviewers other than the data controller to be deleted or returned to data controller within 1 month after an applicant has been offered and accepted the role. For unsuccessful applicants all data to be deleted within 1 year of their application. And for successful applicants within 1 year of leaving the role.

<b>Data Description</b>	<b>Grant applications:</b> Name and private contact details (only when provided as contact details for an organisation).	<b>Allotment tenants' details:</b> Name, contact details, rental payments.	<b>Petitions:</b> Name, postal address and signature.	<b>Publicity data:</b> Names, photographs, varied other personal data as provided.
<b>Data Subject</b>	General public (representative of an organisation seeking a grant).	General public (allotment plot tenants).	General public (individuals who sign a petition that is subsequently submitted to NHPC),	General public.
<b>Purpose and Legal Basis for holding</b>	To contact grant seekers (form content overall used to inform Councillors in the grant approval process).	To manage the rental of NHPC's allotment plots. Public task.	To evidence the level of support amongst Parishioners for the petition in question. Public task.	For publicity purposes (advertising NHPC and community activities). Public task.
<b>Data Controller / (Data Processor)</b>	Parish Clerk.	Allotment Committee Chairman / (Parish Clerk).	NHPC Chairman or Chairman of relevant Committee handling the petition.	Communications Committee Chairman.
<b>Means of obtaining data</b>	NHPC Grant Application Form.	Annual rent demand.	Petition form (N.B. if submitted on a non-standard form NHPC must still accept a petition).	Form CF1.
<b>Data shared with</b>	NHPC Councillors.	NHPC Councillors.	NHPC Councillors and Parish Clerk.	General public.
<b>Length of time data is held</b>	Minimum of 3 years after the end of the financial year in question, and up to 5 years after.	Up to 1 year after the end of the tenancy period, and required for a minimum of 6 months after the completion of the relevant audit process.	Up to 1 year after the submission of the petition.	Indefinitely unless deletion requested by the data subject.

<b>Data Description</b>	<b>Remembrance Day invitees' details:</b> Name, contact details.			
<b>Data Subject</b>	General public (representatives of organisations invited to attend).			
<b>Purpose and Legal Basis for holding</b>	Enabling invitations to be sent out to invitees. Public task.			
<b>Data Controller / (Data Processor)</b>	Parish Clerk.			
<b>Means of obtaining data</b>	No standard form. Usually via the organisation's website, or through personal contacts.			
<b>Data shared with</b>	Remembrance Day Committee members.			
<b>Length of time data is held</b>	Up to 3 years after their last attendance at a Remembrance Day Service.			

**Appendix 2: Consent form CF1 – consent by members of the general public to use contact details on a mailing list and/or to use photographs and/or other personal data for publicity purposes.**

The data controller for this form is the Communications Committee Chairman.



**North Hinksey Parish Council**



CONSENT FORM CF1: INCLUSION IN MAILING LISTS AND/OR USE OF PERSONAL DATA IN NHPC PUBLICITY

Your privacy is important to us and we would like to either (a) communicate with you about the council and its activities, or (b) use your personal data for NHPC publicity purposes. To do either of these we need your consent. Please fill in your name and address and other required information below, and confirm your consent by ticking the relevant boxes.

	Your details	If aged 13 or under your parent or guardian should also fill in their details below to confirm their consent
Name		
Address		
Signature		
Date		

Please confirm your consent below. You can grant consent to any or all of the purposes listed. You can find out more about how we use your data from our “Privacy Notice for the General Public” which is available from our website at <https://northhinksey-pc.gov.uk/about/policies-code-of-conduct/>

You can withdraw or change your consent at any time by contacting the Parish Clerk via [clerk@northhinksey-pc.gov.uk](mailto:clerk@northhinksey-pc.gov.uk) or North Hinksey Parish Council, 3 Church Way, Botley, Oxford OX2 9TH. Please note that requests to delete photographs and other personal data used in newsletters or other printed publicity material may result in the deletion of the original material, but not the deletion of any of the published documents themselves, including e-newsletters or downloadable versions made available online.

<input type="checkbox"/>	We may contact you to keep you informed about what is going on in North Hinksey Parish or other nearby areas including news, events, meetings, clubs, groups and activities. These communications may also sometimes appear on our website, or in printed or electronic form (including social media). Please also tick all relevant boxes below to indicate how you would like us to keep in touch.
<input type="checkbox"/>	We may use your name, photograph and other personal data provided by you in our newsletters, on our website, or our social media accounts (e.g. our Facebook page) or other public communications media. Please list in this box all relevant personal data that you are giving consent to use by means of this consent form:

- Yes please, I would like to receive communications by email
- Yes please, I would like to receive communications by telephone
- Yes please, I would like to receive communications by post

**Appendix 3:** Form CF2 for provision of contact details by NHPC Councillors, and consent to use for specific communication channels.

The data controller for this form is Parish Clerk.



**North Hinksey Parish Council**



**CF2: FORM FOR PROVISION OF NHPC COUNCILLOR/EMPLOYEE/ROLE HOLDER CONTACT DETAILS PLUS CONSENT FORM FOR USE OF COUNCILLOR/EMPLOYEE/ROLE HOLDER DATA FOR PUBLICITY PURPOSES**

This form is to be used for NHPC Councillors, Employees and other Role Holders to provide contact details to the Parish Clerk for internal use on Council matters. N.B. Consent is not required for this purpose. The lawful basis for NHPC retaining this information is ‘public task for the carrying out of official functions’. A postal address, an e-mail address and at least one telephone number is required to enable efficient communications internally between Employees, Councillors and other Role Holders. A portrait photograph (electronic file and hard copy) is also requested to be provided separately by Councillors.

Please fill in these contact details below and sign and date the form.

NHPC Councillor / Employee / Role Holder contact details	
Name	
Address	
E-mail address	
Tel. No. (landline)	
Tel. No. (mobile)	
Signature	
Date	

Please also identify on the rear of this form which elements of your personal data you are willing to allow use of for the various listed types of publicity / communications purposes. N.B. You will be expected to provide consent for at least two types of contact detail (but not just two telephone numbers) per category, plus portrait photographs will normally be placed on the NHPC website. You can find out more about how we use your data from our “Privacy Notice for Councillors, Employees and other Role Holders” which is available on request from the Parish Clerk.

Any additional data provided for specific publicity purposes will require the completion of a consent form CF1, and the “Privacy Notice for the General Public” may also apply (see the NHPC website for a copy).

You can withdraw or change your consent, or provide new contact details at any time by sending an updated copy of this form to the Parish Clerk via [clerk@northhinksey-pc.gov.uk](mailto:clerk@northhinksey-pc.gov.uk) or North Hinksey Parish Council, 3 Church Way, Botley, Oxford OX2 9TH. Please note that requests to delete photographs and other personal data used in newsletters or other printed publicity material may

result in the deletion of the original material, but not the deletion of any of the published documents themselves, including e-newsletters or downloadable versions made available online. Please tick all applicable boxes below to give consent for use of your contact details and portrait photograph in the various types of communications / publicity materials listed below:

	NHPC Website	NHPC Social Media	NHPC Newsletters	Contact List / Other Printed
Name:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Address:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
E-mail address:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Tel. No. (landline):	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Tel. No. (mobile):	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Portrait photograph:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



#### **Appendix 4:** Checklist for dealing with Subject Access Requests (SAR's).

- A. Inform data subjects of their right to access data and provide an easily accessible mechanism through which such a request can be submitted (e.g. a dedicated email address).
- B. Make sure a SAR policy is in place within the council and that internal procedures on handling of SARs are accurate and complied with. Include, among other elements, provisions on:
  - (1) Responsibilities (who, what)
  - (2) Timing
  - (3) Changes to data
  - (4) Handling requests for rectification, erasure or restriction of processing.
- C. Ensure personal data is easily accessible at all times in order to ensure a timely response to SARs and that personal data on specific data subjects can be easily filtered.
- D. Where possible, implement standards to respond to SARs, including a standard response.

#### **21. Upon receipt of a SAR**

- (a) Verify whether you are controller of the data subject's personal data. If you are not a controller, but merely a processor, 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, you 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 you process the data requested. If you do not process any data, inform the data subject accordingly. At all times make sure the internal SAR policy 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.

#### **22. Responding to a SAR**

- (a) 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.
- (c) 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<sup>1</sup> or EU model clauses<sup>2</sup>;
  - (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) Provide a copy of the personal data undergoing processing.

---

<sup>1</sup> “Binding Corporate Rules” is a global data protection policy covering the international transfer of personal data out of the European Union. It requires approval of a data protection regulator in the European Union. In most cases this will be the relevant regulator where an organisation's head quarters is located. In the UK, the relevant regulator is the Information Commissioner's Office.

<sup>2</sup> “EU model clauses” are clauses approved by the European Union which govern the international transfer of personal data. The clauses can be between two data controllers or a data controller and a data processor.