Horsford Parish Council

Data Protection & Data Audit

Policy Contents

CLAUSE

1. Policy statement 1
2. About this policy 1
3. Definition of data protection terms 1
4. Data protection principles 2
5. Fair and lawful processing 3
6. Processing for limited purposes 3
7. Notifying data subjects 3
8. Adequate, relevant and non-excessive processing 4
9. Accurate data 4
10. Timely processing 4
11. Processing in line with data subject's rights 4
12. Data security 5
13. Transferring personal data to a country outside the EEA 5
14. Disclosure and sharing of personal information 6
15. Dealing with subject access requests 7
16. Changes to this policy 7

SCHEDULE

SCHEDULE DATA PROCESSING ACTIVITIES ..... **ERROR! BOOKMARK NOT DEFINED.**

1. POLICY STATEMENT

1.1 Everyone has rights with regard to the way in which their personal data in handled. During the course of our activities we will collect, store and process personal data about our customers, suppliers and other third parties, and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

1.2 Data users are obliged to comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary action.

2. ABOUT THIS POLICY

2.1 The types of personal data that Horsford Parish Councilmay be required to handle include information about current, past and prospective suppliers, customers, and others that we communicate with. The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 1998 (the Act) and other regulations.

2.2 This policy and any other documents referred to in it sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

2.3 This policy does not form part of any employee's contract of employment and may be amended at any time.

2.4 This policy has been approved by Horsford Parish Council it sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

2.5 The Data Protection Compliance Manager is responsible for ensuring compliance with the Act and with this policy. That post is held by the Clerk. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Compliance Manager. Contact by emailing clerk@horsford-pc.gov.uk

3. DEFINITION OF DATA PROTECTION TERMS

3.1 **Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems.

3.2 **Data subjects** for the purpose of this policy include all living individuals about whom we holds personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

3.3 **Personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

3.4 **Data controllers** are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Act. We are the data controller of all personal data used in our business for our own commercial purposes.

3.5 **Data users** are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

3.6 **Data processors** include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on Horsford Parish Council's behalf.

3.7 **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

3.8 **Sensitive personal data** includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

4. DATA PROTECTION PRINCIPLES

Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

(a) Processed fairly and lawfully.

(b) Processed for limited purposes and in an appropriate way.

(c) Adequate, relevant and not excessive for the purpose.

(d) Accurate.

(e) Not kept longer than necessary for the purpose.

(f) Processed in line with data subjects' rights.

(g) Secure.

(h) Not transferred to people or organisations situated in countries without adequate protection.

5. FAIR AND LAWFUL PROCESSING

5.1 The Act is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

5.2 For personal data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in the Act. These include, among other things, the data subject's consent to the processing, or that the processing is necessary for the performance of a contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, or for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, additional conditions must be met. When processing personal data as data controllers in the course of our business, we will ensure that those requirements are met.

6. PROCESSING FOR LIMITED PURPOSES

6.1 In the course of our business, we may collect and process the personal data set out in the **Error! Reference source not found.**. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

6.2 We will only process personal data for the specific purposes set out in the **Error! Reference source not found.** or for any other purposes specifically permitted by the Act. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

7. NOTIFYING DATA SUBJECTS

7.1 If we collect personal data directly from data subjects, we will inform them about:

(a) The purpose or purposes for which we intend to process that personal data.

(b) The types of third parties, if any, with which we will share or to which we will disclose that personal data.

(c) The means, if any, with which data subjects can limit our use and disclosure of their personal data.

7.2 If we receive personal data about a data subject from other sources, we will provide the data subject with this information as soon as possible thereafter.

7.3 We will also inform data subjects whose personal data we process that we are the data controller with regard to that data, and who the Data Protection Compliance Manager is.

8. ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

9. ACCURATE DATA

We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

10. TIMELY PROCESSING

We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

11. PROCESSING IN LINE WITH DATA SUBJECT'S RIGHTS

We will process all personal data in line with data subjects' rights, in particular their right to:

(a) Request access to any data held about them by a data controller (see also clause 15).

(b) Prevent the processing of their data for direct-marketing purposes.

(c) Ask to have inaccurate data amended (see also clause 9).

(d) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

12. DATA SECURITY

12.1 We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

12.2 We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

12.3 We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

(a) **Confidentiality** means that only people who are authorised to use the data can access it.

(b) **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.

(c) **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on Horsford Parish Council's central computer system instead of individual PCs.

12.4 Security procedures include:

(a) **Entry controls.** Any stranger seen in entry-controlled areas should be reported.

(b) **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

(c) **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.

(d) **Equipment.** Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

13. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

13.1 We may transfer any personal data we hold to a country outside the European Economic Area ("EEA"), provided that one of the following conditions applies:

(a) The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms.

(b) The data subject has given his consent.

(c) The transfer is necessary for one of the reasons set out in the Act, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject.

(d) The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.

(e) The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

13.2 Subject to the requirements in clause 12.1 above, personal data we hold may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. That staff maybe engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

14. DISCLOSURE AND SHARING OF PERSONAL INFORMATION

14.1 We may share personal data we hold with any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries, as defined in section 1159 of the UK Companies Act 2006.

14.2 We may also disclose personal data we hold to third parties:

(a) In the event that we sell or buy any business or assets, in which case we may disclose personal data we hold to the prospective seller or buyer of such business or assets.

(b) If we or substantially all of our assets are acquired by a third party, in which case personal data we hold will be one of the transferred assets.

14.3 If we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

14.4 We may also share personal data we hold with selected third parties for the purposes set out in the **Error! Reference source not found.**.

15. DEALING WITH SUBJECT ACCESS REQUESTS

15.1 Data subjects must make a formal request for information we hold about them. This must be made in writing. Employees who receive a written request should forward it to the Clerk, the Data Protection Compliance Manager immediately.

15.2 When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:

(a) We will check the caller's identity to make sure that information is only given to a person who is entitled to it.

(b) We will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

15.3 Our employees will refer a request to their line manager [or the Data Protection Compliance Manager] for assistance in difficult situations. Employees should not be bullied into disclosing personal information.

16. CHANGES TO THIS POLICY

We reserve the right to change this policy at any time. Where appropriate, we will notify data subjects of those changes by mail or email.

Data Audit

Category	Document Type	Personal Details Held	Purpose	Legal Basis	Shared With	Purpose for Sharing	How it is held	Length of time to be held
Employees	HR Records - contract, references, application form	Contact details, NI number, employment history, pension records	For setting up and management employment of staff	Legal obligation	Not shared	n/a	Electronically/hard copy	6 years after period of employment has ceased with the Parish Council
	CV's and job applications	Contact and personal details, employment history	Recruitment	Public task	Not shared	n/a	Electronically/ hard copy	6 months after notifying unsuccessful applicant
	Payment of salaries	Bank details	Payment of salaries	Legal obligation	Parish Council bank signatories	Authorise payment	Electronically/hard copy	Duration of employment
Councillors	Contact details	Name, address, telephone number, email address	Public, democracy	Legal obligation Public task Consent	Councillors, Public	Public information	Electronically/hard copy/website	Term of office

	Application for co-option	Name, address, telephone number, email address and other personal details e.g. why they wish to become a Councillor	Public, democracy	Public task	Not shared	n/a	Electronically/hard copy	3 months after vacancy has been filled
	Declaration of interest form	Pecuniary and other interests	Legal requirement	Legal Obligation Public Task	On BDC website with a link from the Parish Council's website	Public information	On District Council's website with link to the Parish Council's website	Term of office (Parish Council copy)
Members of the public	Electoral register	Name, address	Reference	Public Task	Not shared – Broadland District Council share this with the Clerk upon request	N/A	N/A	Current year only
	Correspondence - letters/emails	Contact details	To request information, pass on information of make a statement	Public Task (Article 6(1)(e) UK GDPR)	Councillors (where necessary) Other Authorities (with permission)	To assist in resolving queries	Electronically/ hard copy	For as long as is necessary

	Contact details of those involved in local groups	Name, address, telephone number, email address	Council business	Public	Councillors (where necessary) Other Authorities (with permission)	Council business	Informed - email and website	Until Parish Council are informed that they are no longer involved with the group
	Allotment tenants	Contact and signature details on Tenancy Agreement	Contractual	Contract	Not shared	N/A	Electronically/hard copy	For up to 7 years after plot vacated for auditing purposes
	Allotment waiting list	Contact details	Prospective tenant	Contract	Not shared	N/A	Electronically/hard copy	Until allocated a plot or request to be removed received by Council.
	Grant applications	Name, address, telephone number, email address, reason for requesting grant, other relevant details about the organisation/local group requesting grant	To consider requests for grants from local non-profit making organisations	Legal obligation (UK GDPR) Article 6(1)(c) Public task (UK GDPR) Article 6(1)(e)	Not shared	Council business	n/a	If successful - 7 years for auditing purposes. If unsuccessful - 1 year

Contractors	Contractors providing goods or services to the Parish Council	Contact details, details of the contract between the two parties	Contractual	Legal obligation (UK GDPR) Article 6(1)(c) Public task (UK GDPR) Article 6(1)(e)	Councillors (if appropriate)	Council business	Informed - email and website	Life of contract and up to 12 years thereafter
	Quotes and tenders	Name, address, telephone number, email address, references	Council business	Legal obligation (UK GDPR) Article 6(1)(c) Public task (UK GDPR) Article 6(1)(e)	Councillors (if appropriate), Internal Auditor, Public Inspection (Audit)	Council business	Informed - email and website	12 years
	Invoices	Good/services received/supplied	As a record for financial purposes, audit and annual return	Legal obligation (UK GDPR) Article 6(1)(c) Public task (UK GDPR) Article 6(1)(e)	Councillors (if appropriate), Internal Auditor, Public Inspection (Audit)	Council business	Informed - email and website	6 years