Waldringfield Parish Council

Data Protection and Information Management Policy

Adopted 14 November 2023

Waldringfield Parish Council

Data Protection and Information Management Policy

1. Introduction

1.1. This policy outlines the standards Waldringfield 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, and photographs.

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 or volunteers, 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.

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

2.4. 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 by employees or volunteers may result in disciplinary action in accordance with the Council's employment 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.

3.2. Councillors found to be in breach of this policy may also be deemed to have breached the Council's adopted Code of Conduct and referred to the Monitoring Officer for East Suffolk Council.

4. Privacy

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.

4.3. The Council's Data Privacy Notice is available on the Council's website and is at **Appendix A.**

5. Contracts

5.1. The Council acknowledges that 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

5.5. Council officer must ensure that personal data is managed in accordance with data protection law and this Policy.

5.6. 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.

5.7. Council officers will use the appropriate processes and templates 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. Individual 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).

7.2. Individuals also have other rights under the Data Protection Act 2018 which are set out in the Council's privacy notice (**at Appendix A**). 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.

9.3. The Council will fully investigate both actual and potential failures and take remedial steps if necessary. If the incident involves or impacts personal data it must be reported to the ICO within 72 hours.

10. IT and Communication 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.

10.3. Equipment security and passwords

10.3.1 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.

10.4. Systems and data security

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

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

10.4.3. 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.

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

10.5 Email

10.5.1. Users should adopt a professional tone and observe appropriate etiquette

when communicating with third parties by e-mail.

10.5.2. 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.

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

10.5.4. 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.

10.6. Using the Internet

10.1.1. 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.

10.1.2. 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.

10.7. Prohibited use of Council systems

10.7.1. 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.

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

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

10.7.4. offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or our local community;

10.7.5. a false and defamatory statement about any person or organisation;

10.7.6. material which is discriminatory, offensive, derogatory or may cause embarrassment to others (including material which breaches the Council's Equality and Diversity Policy);

10.7.7. confidential information about the Council or any of our staff or our

community (except as authorised in the proper performance of your duties);

10.7.8. unauthorised software;

10.7.9. any other statement which is likely to create any criminal or civil liability; or

10.7.10. music or video files or other material in breach of copyright.

11. Social Media

11.1. This policy is in place to minimise the risks to the Council through use of personal social media. The Council does not at this time have a social media account.

11.2. This policy deals with the use of all forms of social media, including Facebook, LinkedIn, Twitter, Google+, Wikipedia, Instagram, WhatsApp and all other social networking sites, internet postings and blogs. It applies to use of social media for Council purposes as well as personal use that may affect our business in any way.

11.3. Prohibited use

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

11.3.2. 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.

11.3.3. Any misuse of social media should be reported to the Clerk.

11.4. Guidelines for responsible use of social media

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

11.4.2. 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.

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

11.4.4. 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.

11.5. Bring your own device (BYOD)

11.5.1. 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.

11.5.2. 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.
- Users will enable a security pin to access their device and an automatic lock every 5 minutes requiring re-entry of the pin.
- Users will ensure security software is set up on their device and kept up to date.
- Users will not use their device to store Council emails, files and data.

12. Records Management

It is necessary for the Council to retain a number of data sets and records as part of managing council business and meeting obligations under other relevant legislation The Council shall apply the following framework :

Document(s)	Minimum Retention	Reason
Minute books	Indefinite	Archive
Scales of fees and charges	6 years	Management
Receipt and payment account(s)	Indefinite	Archive

Receipts and receipt books of all kinds	6 years	VAT
Bank statements, including deposit/savings accounts	Last completed audit year	Audit
Bank paying-in books	Last completed audit year	Audit
Cheque book stubs	Last completed audit year	Audit
Quotations and tenders	6 years	Limitation Act 1980 (as amended)
Paid invoices	6 years	VAT
Paid cheques	6 years	Limitation Act 1980 (as amended)
VAT records	6 years generally but 20 years for VAT on rents	VAT
Petty cash, postage and telephone books	6 years	Tax, VAT, Limitation Act 1980 (as amended)
Timesheets	Last completed audit year 3 years	Audit (requirement) Personal injury (best practice)
Wages books	12 years	Superannuation
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.
Investments	Indefinite	Audit, Management
Title deeds, leases, agreements, contracts	Indefinite	Audit, Management
Members allowances register	6 years	Tax, Limitation Act 1980 (as amended)
For Halls, Centre, Recreation Grounds (Currently not applicable)		

▪ application to hire ▪ lettings diaries ▪ copies of bills to hires ▪ record of tickets issued	6 years	VAT
For Allotments (Currently not applicable)		
Tenancy Agreement, register and plans	Indefinite	Audit, Management
For Burial Grounds (Currently not applicable)		
▪ register of fees collected ▪ register of burials ▪ register of purchased graves ▪ register/plan of grave spaces ▪ register of memorials ▪ applications for interment ▪ applications for right to erect memorials ▪ disposal certificates ▪ copy certificates of grant of exclusive right of burial	Indefinite	Archives, Local Authorities Cemeteries Order 1977 (SI. 204)

APPENDIX A

DATA PRIVACY NOTICE

Waldringfield Parish Council

Introduction

The General Data Protection Regulation ('GDPR'), governing the processing of personal data came into effect on the 25th May 2018. Waldringfield Parish Council ('the Council') must comply with its requirements, just like any other organisation. A description of what personal data the Council processes and for what purposes is set out in this Privacy Notice. It also describes your rights with regard to personal data WPC holds.

It is with design that the Council only holds the minimum data necessary to carry out its duties, and will always endeavour to process that data lawfully, keep it secure and uphold your rights over your personal data, as described below.

Your personal data – what is it?

"Personal data" is any information about a living individual which allows them to be identified from that data (for example a name, photographs, videos, email address, or address). Identification can be directly using the data itself or by combining it with other information which helps to identify a living individual.

Who are we?

This Privacy Notice is provided to you by the Council, which is the data controller for your data. This means it decides how your personal data is processed and for what purposes.

Other data controllers the Council works with

We may need to share your personal data we hold with other organisations so that they can carry out their responsibilities to the Council. 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 to you for your data.

Where each of the parties are processing your data for their own independent purposes then each of us will be independently responsible to you and if you have any questions, wish to exercise any of your rights (see below) or wish to raise a complaint, you should do so directly to the relevant data controller.

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

- Names, titles, and aliases, photographs
- Contact details such as telephone numbers, addresses, and email addresses
- Where they are relevant to the services provided by the Council, or where you provide them to us, we may process information such as gender, age, marital status, nationality, education/work history, academic/professional qualifications, hobbies, family composition, and dependants

The reasons for processing the different types of data, and the legal basis for processing them are shown below:

Type of Data	Purpose	Legal Basis of Processing
Name, address, phone number, email address	Communication with member of the public	**Public task**. Parish Councils have a statutory obligation to communicate with members of the public, to keep them informed of parish issues and address parishioners' concerns.
Name, address, phone number, email address	List of deliverers of the parish newsletter	**Public task**. As above.
Name, company address, company phone number, company email address	Communication with company providing services to WPC.	**Contract**. Parish Councils need to pay for services to fulfil their legal obligations to maintain council facilities, e.g. grass cutting, play equipment maintenance.
Name, organisation's address, organisation's phone number, organisation's email address	Communication with officer or member of local government organisation (e.g. SCC, SCDC, AONB, DEP, etc.)	**Public task**. Parish Councils need to communicate with officers or members of local government organisations, e.g. on planning issues.

The Council will comply with data protection law. This says that the personal data we hold about individuals must be:

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

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

- To deliver public services and to understand and inform individuals of other relevant services
- To confirm identity to provide some services

- To contact individuals by post, email, telephone
- To help us to build up a picture of how we are performing
- To prevent and detect fraud and corruption in the use of public funds and where necessary for the law enforcement functions
- To enable us to meet all legal and statutory obligations and powers including any delegated functions
- To carry out comprehensive safeguarding procedures (including due diligence and complaints handling) in accordance with best safeguarding practice from time to time with the aim of ensuring that all children and adults-at-risk are provided with safe environments and generally as necessary to protect individuals from harm or injury
- To promote the interests of The Council
- To maintain our own accounts and records
- To seek your views, opinions or comments
- To notify individuals of changes to our facilities, services, events and staff, councillors and other role holders
- To send you communications that may be of interest to residents or individuals. 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.

What is the legal basis for processing your personal data?

The Council is a public authority and has certain powers and obligations. Most personal data is processed for compliance with a legal obligation which includes the discharge of the Council's statutory functions and powers.

Sometimes when exercising these powers or duties it is necessary to process personal data of residents or individuals using the Council's services. We will always take into account your interests and rights. This Privacy Notice sets out your rights and WPC's obligations to you.

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

Sharing your personal data

This section provides information about the third parties with whom the Council may share personal data. These third parties have an obligation to put in place appropriate security measures and will be responsible to individuals directly for the manner in which they process and protect your personal data.

It is possible that the Council may need to share your data with some or all of the following (but only where necessary):

- Our agents, suppliers and contractors. For example, we may ask a commercial provider to publish or distribute newsletters on our behalf.
- On occasion, other local authorities or not for profit bodies with which we are carrying out joint ventures e.g. in relation to facilities or events for the community.

How long do we keep your personal data?

The Council 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.

The Council 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).

The Council will retain some personal data for this purpose as long as it believes it is necessary to be able to defend or pursue a claim. In general, the Council will endeavour to keep data only for as long as we need it. This means that the Council will delete it when it is no longer needed.

Individual rights and your personal data

Individuals have the following rights with respect to their personal data:
When exercising any of the rights listed below, in order to process a request, the Council may need to verify identity for requester's security. In such cases the Council will need requestors' to respond with proof of identity before you can exercise these rights.

1) The right to access personal data we hold on you

At any point you can contact us to request the personal data we hold on you as well as why we have that personal data, who has access to the personal data and where we obtained the personal data from. Once we have received your request we will respond within one month.

There are no fees or charges for the first request but additional requests for the same personal data or requests which are manifestly unfounded or excessive may be subject to an administrative fee.

2) The right to correct and update the personal data we hold on you

If the data we hold on you is out of date, incomplete or incorrect, you can inform us and your data will be updated

3) The right to have your personal data erased

If you feel that we should no longer be using your personal data or that we are unlawfully using your personal data, you can request that we erase the personal data we hold. When we receive your request we will confirm whether the personal data has been deleted, or the reason why it cannot be deleted (for example because we need it to comply with a legal obligation.

4) The right to object to processing of your personal data or to restrict it to certain purposes only

You have the right to request that we stop processing your personal data or ask us to restrict processing. Upon receiving the request we will contact you and let you know if we are able to comply or if we have a legal obligation to continue to process your data.

5) The right to data portability

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

6) The right to withdraw your consent to the processing at any time for any processing of data to which consent was obtained

You can withdraw your consent easily by telephone, email, or by post (see Contact Details below)

7) The right to lodge a complaint with the Information Commissioner's Office.

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

Transfer of Data Abroad

The Council has no reason to believe it would require data to be transferred overseas. However, should this be required in future, 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.

Further processing

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

Changes to this notice

We keep this Privacy Notice under regular review and we will place any updates on this web page http://waldringfield.onesuffolk.net/parish-council/council-documents-online/ . This Notice was last updated in October 2023.

Contact Details

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

Jennifer Shone-Tribley (Clerk to the Council & Responsible Financial Officer)
Low Farm, Ipswich Road, Waldringfield, Woodbridge, Suffolk IP12 4QU
Email: pc.waldringfield@googlemail.com
Tel: 01473 736475 (with voicemail)