



EDITH WESTON PARISH COUNCIL

Data Protection/GDPR Policy

Purpose

Edith Weston Parish Council (EWPC) is committed to being transparent about how it collects and uses the personal data of staff, and to meeting our data protection obligations. This policy sets out EWPC's commitment to data protection, and your rights and obligations in relation to personal data in line with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA).

This policy applies to the personal data of current and former job applicants, employees, workers, contractors, and former employees, referred to as HR-related personal data. This policy does not apply to the personal data relating to members of the public or other personal data processed for council business.

EWPC has appointed Parish Councillor Joseph Akak as the person with responsibility for data protection compliance (Data Protection Officer (DPO)) within EWPC. Questions about this policy, or requests for further information, should be directed to them.

Definitions

- "Personal data" is any information that relates to a living person who can be identified from that data (a 'data subject') on its own, or when taken together with other information. It includes both automated personal data and manual filing systems where personal data are accessible according to specific criteria. It does not include anonymised data.
- "Processing" is any use that is made of data, including collecting, recording, organising, consulting, storing, amending, disclosing or destroying it.
- "Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic or biometric data as well as criminal convictions and offences.
- "Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Data protection principles

EWPC processes HR-related personal data in accordance with the following data protection principles:

- lawfully, fairly and in a transparent manner
- collected only for specified, explicit and legitimate purposes
- collected only where it is adequate, relevant and limited to what is necessary for the purposes of processing

EWPC Data Protection/GDPR Policy – approved July 2023, minute no: 130/23; reviewed July 2024, minute no: 059/24

- keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay
- keeps personal data only for the period necessary for processing
- adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

EWPC will tell you of the personal data it processes, the reasons for processing your personal data, how we use such data, how long we retain the data, and the legal basis for processing in our privacy notices.

EWPC will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it. EWPC will not process your personal data if it does not have a legal basis for processing.

EWPC keeps a record of our processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

Processing

1. Personal data

EWPC will process your personal data (that is not classed as special categories of personal data) for one or more of the following reasons:

- it is necessary for the performance of a contract, e.g., your contract of employment (or services); and/or
- it is necessary to comply with any legal obligation; and/or
- it is necessary for EWPC's legitimate interests (or for the legitimate interests of a third party), unless there is a good reason to protect your personal data which overrides those legitimate interests; and/or
- it is necessary to protect the vital interests of a data subject or another person; and/or
- it 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.

If EWPC processes your personal data (excluding special categories of personal data) in line with one of the above bases, it does not require your consent. Otherwise, EWPC is required to gain your consent to process your personal data. If EWPC asks for your consent to process personal data, then we will explain the reason for the request. You do not need to consent or can withdraw consent later.

EWPC will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.

Personal data gathered during the employment is held in your personnel file in hard copy and electronic format on HR and IT systems and servers. The periods for which EWPC holds your HR-related personal data are contained in our privacy notices to individuals.

Sometimes EWPC will share your personal data with contractors and agents to carry out our obligations under a contract with the individual or for our legitimate interests. We require those individuals or companies to keep your personal data confidential and secure and to protect it in accordance with Data Protection law and our policies. They are only permitted to process that data for the lawful purpose for which it has been shared and in accordance with our instructions.

EWPC will update HR-related personal data promptly if you advise that your information has changed or is inaccurate. You may be required to provide documentary evidence in some circumstances.

EWPC keeps a record of our processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

2. Special categories of data

EWPC will only process special categories of your personal data (see above) on the following basis in accordance with legislation:

- where it is necessary for carrying out rights and obligations under employment law or a collective agreement;
- where it is necessary to protect your vital interests or those of another person where you are physically or legally incapable of giving consent;
- where you have made the data public;
- where it is necessary for the establishment, exercise or defence of legal claims;
- where it is necessary for the purposes of occupational medicine or for the assessment of your working capacity;
- where it is carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates to only members or former members provided there is no disclosure to a third party without consent;
- where it is necessary for reasons of substantial public interest on the basis of law which is proportionate to the aim pursued and which contains appropriate safeguards;
- where it is necessary for reasons of public interest in the area of public health; and
- where it is necessary for archiving purposes in the public interest or scientific and historical research purposes.

If EWPC processes special categories of your personal data in line with one of the above bases, it does not require your consent. In other cases, EWPC is required to gain your consent to process your special categories of personal data. If EWPC asks for your consent to process a special category of personal data, then we will explain the reason for the request. You do not have to consent or can withdraw consent later.

Individual rights

As a data subject, you have a number of rights in relation to your personal data.

1. Subject access requests

You have the right to make a subject access request. If you make a subject access request, EWPC will tell you:

- whether or not your data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from yourself;
- to whom your data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long your personal data is stored (or how that period is decided);
- your rights to rectification or erasure of data, or to restrict or object to processing;
- your right to complain to the Information Commissioner if you think EWPC has failed to comply with your data protection rights; and
- whether or not EWPC carries out automated decision-making and the logic involved in any such decision-making.

EWPC will also provide you with a copy of your personal data undergoing processing. This will normally be in electronic form if you have made a request electronically, unless you agree otherwise.

If you want additional copies, EWPC may charge a fee, which will be based on the administrative cost to EWPC of providing the additional copies.

To make a subject access request, you should send the request to the DPO of EWPC. In some cases, EWPC may need to ask for proof of identification before the request can be processed. EWPC will inform you if we need to verify your identity and the documents we require. EWPC will normally respond to a request within a period of one month from the date it is received. Where EWPC processes large amounts of your data, this may not be possible within one month. EWPC will write to you within one month of receiving the original request to tell you if this is the case.

If a subject access request is manifestly unfounded or excessive, EWPC is not obliged to comply with it. Alternatively, EWPC can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which EWPC has already responded. If you submit a request that is unfounded or excessive, EWPC will notify you that this is the case and whether or not we will respond to it.

2. Other rights

You have a number of other rights in relation to your personal data. You can require EWPC to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if your interests override EWPC's legitimate grounds for processing data (where EWPC relies on our legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not your interests override EWPC's legitimate grounds for processing data.

EWPC Data Protection/GDPR Policy – approved July 2023, minute no: 130/23; reviewed July 2024, minute no: 059/24

- complain to the Information Commissioner. You can do this by contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk).

To ask EWPC to take any of these steps, you should send the request to the DPO of EWPC.

Data security

EWPC takes the security of HR-related personal data seriously. EWPC has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

Where EWPC engages third parties to process personal data on our behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

1. Data breaches

EWPC have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur EWPC must take notes and keep evidence of that breach. If you are aware of a data breach you must contact the DPO of EWPC immediately and keep any evidence, you have in relation to the breach.

If EWPC discovers that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of yourself, we will report it to the Information Commissioner within 72 hours of discovery. EWPC will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, we will tell you that there has been a breach and provide you with information about its likely consequences and the mitigation measures we have taken.

2. International data transfers

EWPC will not transfer HR-related personal data to countries outside the EEA.

3. Individual responsibilities

You are responsible for helping EWPC keep your personal data up to date. You should let EWPC know if data provided to EWPC changes, for example if you move to a new house or change your bank details.

Everyone who works for, or on behalf of, EWPC has some responsibility for ensuring data is collected, stored and handled appropriately, in line with EWPC's policies.

You may have access to the personal data of other individuals and of members of the public in the course of your work with EWPC. Where this is the case, EWPC relies on you to help meet our data

protection obligations to staff and members of the public. Individuals who have access to personal data are required:

- to access only data that you have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside EWPC) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, locking computer screens when away from desk, and secure file storage and destruction including locking drawers and cabinets, not leaving documents on desk whilst unattended);
- not to remove personal data, or devices containing or that can be used to access personal data, from EWPC's premises without prior authorisation and without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for work purposes.
- to never transfer personal data outside the European Economic Area except in compliance with the law and with express authorisation from the Clerk or Chair of EWPC
- to ask for help from EWPC's data protection lead if unsure about data protection or if you notice a potential breach or any areas of data protection or security that can be improved upon.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under EWPC's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing personal data without authorisation or a legitimate reason to do so or concealing or destroying personal data as part of a subject access request, may constitute gross misconduct and could lead to dismissal without notice.

This is a non-contractual policy and procedure which will be reviewed annually (last review May 2022, minute no. 84/22).

Notes

1. Data audit

It is important that EWPC's policy reflects current practice. Any policy must be based on a data audit to ensure that EWPC understands what data is collected, where it is stored, who has access to the data and the measures taken to ensure it is secure. For more information on implementing a Data Protection Policy, please refer to the Information Commissioner website.

2. Data Protection Officer

The policy assumes that EWPC has a Data Protection lead rather than appointed a Data Protection Officer (DPO). The role of DPO is set out in legislation and infers specific obligations. Parish councils in England and community councils in Wales and Scotland are exempt from having to appoint a DPO (<https://ico.org.uk/for-organisations/in-your-sector/local-government/local-gov-gdpr-faqs/>) but are still subject to data protection legislation and must ensure sufficient resources to meet the obligations under the GDPR.

3. Data storage within the EU

You need to take account of where your data is stored including servers, on the cloud, and where your suppliers might hold their data including on their server.

EWPC Data Protection/GDPR Policy – approved July 2023, minute no: 130/23; reviewed July 2024, minute no: 059/24

Appendix 1 – Document Retention Policy

Nature of Information or documentation	Typical retention period
Class 1 - Who we are and what we do - (Organisational information, structures, locations and contacts)	
1.1 Organisational information, structures, locations and contacts	Current information
1.2 Who's who on the Council and its committees	Current information
1.3 Contact details for Parish Clerk and Council	Current information
1.4 Location of main Council office and accessibility details	Current information
1.5 Staffing structure	Current information
Class 2 – What we spend and how we spend it - (Financial information relating to projected and actual income and expenditure, procurement, contracts and financial audit)	
2.1 Annual return form and report by auditor	6 complete years
2.2 Finalised budget	6 complete years
2.3 Precept	6 complete years
2.4 Borrowing approval letters	6 complete years
2.5 Financial standing orders and regulations	Current and previous years
2.6 Grants given and received	6 complete years
2.7 List of current contracts awarded and value of contracts	6 complete years
2.8 Members' allowances and expenses	6 complete years
2.9 Vouchers including VAT records, petty cash and bank statements	6 complete years
2.10 Receipts and payments accounts and balance sheets	Indefinite
2.11 Bank paying in books, cheque stubs	1 complete year
2.12 Scales of fees and charges	5 years
2.13 Quotations and tenders	12 years
2.14 Timesheets	1 complete year
2.15 Wages and salary records	6 complete years
2.16 Insurance policies	Current information
2.17 Investments	6 complete years
2.18 Deeds, leases etc	Indefinite
Class 3 – What our priorities are and how we are doing – (strategies and plans, performance indicators, audits, inspections and reviews)	
3.1 Annual Report to Parish or Community Meeting	Indefinite
3.2 Parish Plan	Not applicable
3.3 Quality Status/Local Council Awards Scheme	Not applicable
3.4 Local charters	Not applicable
Class 4 – How we make decisions – (decision making processes and records of decisions)	
4.1 Timetable of meetings (council, any committee/sub-committee	Current information

EWPC Data Protection/GDPR Policy – approved July 2023, minute no: 130/23; reviewed July 2024, minute no: 059/24

meetings and parish meetings)	
4.2 Agendas of meetings	2 years
4.3 Minutes of meetings	Indefinite
4.4 Reports presented to council	2 years
4.5 Responses to consultation papers	2 years
4.6 Responses to planning applications	Not applicable (held by RCC)
4.7 By-laws	Current information
Class 5 – Our policies and procedures – (current written protocols, policies and procedures for delivery our services and responsibilities)	
5.1 Policies and procedures for the conduct of council business: <ul style="list-style-type: none"> • Procedural standing orders • Committee and sub-committee terms of reference • Delegated authority in respect of officers (see Standing orders) • Code of Conduct • Policy statements • All other policies and procedures • Clerk’s ‘aide memoire’ recordings of meetings 	Current information Current information Current information Current information Current information Current information Following approval of the minutes by the Parish Council, recordings will be deleted
Class 6 – Lists and Registers – (currently maintained lists and registers only (some information may only be available by inspection))	
6.1 Assets Register	Current information
6.2 Register of members’ interests	Indefinite
6.3 Register of gifts and hospitality	Indefinite
6.4 Declaration of acceptance of office	Indefinite
6.5 Electoral register (older version available from Rutland County Council)	Current information – not to be disclosed
Class 7 – The services we offer – (information about the services we offer, including leaflets, guidance and newsletters produced for the public and businesses)	
Not applicable	