ST MABYN PARISH COUNCIL

DATA PROTECTION POLICY

Purpose

St Mabyn Parish Council is committed to being transparent about how it collects and uses the personal data of staff, service providers and members of the public, and to meeting its data protection obligations. This policy sets out the Council's commitment to data protection, and your rights and obligations in relation to personal data in line with the General Data Protection Regulations (GDPR) and the Data Protection Act 2018 (DPA). The Act regulates the use of personal data. This does not have to be sensitive data; it can be as little as a name and address.

The Council has appointed the Clerk as the person with the responsibility for data protection compliance within the Council. Questions about this policy, or request for further information, should be directed to the Clerk.

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 is accessible according to specific criteria. It does not include anonymous 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

The Council processes personal data in accordance with the following data protection principles of the Council:

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

The Council 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.

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

The Council keeps a record of our processing activities in respect of HR related personal data in accordance with the requirements of GDPR.

Processing Personal Data

The Council will process your personal data (that is 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., a contract of employment or for services provided; and/or
- It is necessary to comply with any legal obligation; and/or
- It is necessary for the Council'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 if a task carried out in the public interest or in the exercise of official authority vested in the controller.

If the Council 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 the Council is required to gain your consent to process your personal data. If the Council asks for your consent to process personal data, then it will explain the reason for the request. You do not need to consent or can withdraw consent later.

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

Personal data gathered during an employment is held in a Personnel file in hard copy and electronic format on HR and IT systems and servers. The period for which the Council holds HR-related personal data is contained in its privacy notices to individuals.

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

The Council will update HR related personal data promptly when advised that information is changed or inaccurate. In some circumstances documentary evidence will be required. The Council keeps a record of its processing activities in respect of HR related personal data in accordance with the requirements of GDPR.

Special categories of data

The Council will only process special categories of personal data on the following basis of legislation:

- Where it is necessary for carrying out rights and obligations under employment law or 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 the assessment of employees working capacity
- Where it I 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 the Council processes special categories of your personal data in line with one of the above bases, it does not require your consent. In other cases the Council is required to gain your consent to process your special categories of personal data/

If the Council asks for your consent to process a special category of personal data, then the reason for the request will be explained. 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.

Subject Access Requests (SAR)

You have the right to make a Subject Access Request (SAR). If you make a SAR the council will tell you:

- Whether or not your data is process 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 o to object to processing;
- Your right to complain to the Information Commissioner if you think the Council has failed to comply with your data protection rights; and
- Whether or not the Council carries out automated decision-making and the logic in any such decision making.

The Council 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 the Council may charge a fee, which will be based on the administrative cost to the Council of providing the additional copies.

To make a SAR you should send the request to the Clerk or Chairman of the Council. In some cases the Council may need to ask for proof of identification before the request can be processed. The Council will inform you if it needs to verify your identity and the documents required.

The Council will normally respond to a SAR request within one month from the date it is received. Where the Council processes large amounts of your data this may not be possible within one month. The Council will write to you within one month of receiving the original request if this is the case.

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

Other rights

You have a number of other rights in relation to your personal data. You can require the Council 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 the Council's legitimate grounds for processing data (where the Council relies on its 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 the Council's legitimate grounds for processing data.
- 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 the council to take any of the above steps you should send the request to the Clerk or Chairman of the Council.

Data Security

The Council takes the security of personal data seriously. The Council has internal policies and internal 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 the Council engages third parties to process personal data on its 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.

Data Breaches

The Council has robust measures in place to minimise and prevent data breaches from taking place. If a breach of personal data occurs the Council must take notes and keep evidence of that breach. If you are aware of a data breach you must contact the Clerk or Chairman of the Council immediately and keep any evidence you have in relation to the breach.

If the Council discovers that there has been a breach of HR related personal data that poses a risk to the rights and freedoms of the individual concerned it will be reported to the Information Commissioner within 72 hours of discovery. The Council 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 it will tell you that there has been a breach and provide you with information about its likely consequences and the mitigation measures that it has taken.

International data transfers

The council will not transfer personal data to countries outside the EAA.

Individual Responsibilities of Staff

The Clerk is responsible for helping the Council keep his/her personal data up to date. The Council should be notified if data provided changes, for example a change of address or bank details. Everyone who works for, or on behalf of, the council has some responsibility for ensuring data is collected, stored and handled appropriately and in line with the Council's policies.

The Clerk will have access to the personal data of other individuals and of members of the public in the course of his/her work with the Council. The Council relies on him/her to help meet its 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 of the Council) 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 not in use and secure file storage and destruction including locking drawers and cabinets and not leaving documents unattended;
- Not to remove personal data or devices that can be used to access personal data from the normal place of work without prior authorisation and without adopting the 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 is 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 Council.

Failing to observe the above requirements may amount to a disciplinary offence which will be dealt with under the Council'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.

Adopted: 3rd March 2026