SWAFFHAM PRIOR PARISH COUNCIL

DATA PROTECTION POLICY

Purpose.

Swaffham Prior Parish Council are 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 the council'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.

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 and to personal data relating to members of the public and other personal data processed for council business.

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

Definitions.

"Personal data" is any information which 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 anonymised data.

"Processing" is any use that is made of data, including collecting, recording, organising, consulting, storing, amending, disclosing and 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 person data in accordance with the following data protection principles. 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 reason 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 policy.

The Council 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. The Council will not process your personal data if it does not have a legal basis for processing.

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

Processing.

Personal data.

The Council will process your personal data (that is not classified 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 of services) and/or
- it is necessary to comply with a 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 good reason to protect your personal data which overrides those legitimate interest 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 ot 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 the reason for the request will be explained. 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 we intend to rely on for processing it.

Personal data gathered during employment is held in your personnel file in hard copy and electronic format on HR and IT systems and servers. The periods for which the Council holds personal data are contained in our privacy policy and retention policy.

Sometimes the Council 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 the data for the lawful purpose for which it has been shared and in accordance with our instructions.

The Council will update personal promptly if you advise that your information has changed or is inaccurate. You may be required to provide documentary evidence in some circumstances.

Special categories of data.

The Council will only process special categories of your personal data (see above) on the following basis according to 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 contain 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 you special categories of personal data. If the Council askes for your consent to process a special category of personal data, then it will explain the reason for the request. You do not have to consent and 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.

You have the right to make a subject access request. If you make a subject access request, the Council 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 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 the Council has failed to comply with your data protection rights
- whether or not the Council carries out automated decision-making and the logic involved 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 additional copies.

To make a subject access request, you should send the request to the Clerk or the Chair 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 verification of your identity is needed and of the documents required.

The Council will normally respond to a request within a period of 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 tell you within one month of the original request if this is the case.

If the subject access request is manifestly unfounded or excessive, the Council is not obliged to comply with it. Alternatively the Council can agree to respond but charge a fee, which is 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 the Council has already responded. If you submit a request which is manifestly unfounded or excessive, the Council will notify you that this is the case and whether or not it will respond.

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 purpose of processing
- stop processing or erase data if your interests override the Council's legitimate grounds for processing data (where the Council relies on legitimate grounds for processing data)
- stop processing or erase data if processing is unlawful
- stop processing 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.

To ask the Council to take any of these steps, you should send the request to the Clerk or Chair of the Council.

You can also 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.

Data security.

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

Where the Council engage third parties to process personal data on its behalf, such third 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 have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur, the Council must take notes and keep evidence of the breach.

If you are aware of a data breach you must contact the Clerk or the Chair of the Council immediately and keep any evidence you have in relation to the breach.

If the Council discovers there has been a breach of personal data that poses a risk to the rights and the freedoms of yourself, 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, the Council will tell the individuals concerned that there has been a breach and provide them with information about its likely consequences and the mitigation measures taken.

International data transfers.

The Council will not transfer personal data to countries outside the EEA.

Individual responsibilities.

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

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

Council members and employees may have access to the personal data of other individuals and of members of the public in the course of work for the Council. Where this is the case, the Council relies on employees to help meet its 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 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 away from desk, secure file storage and destruction, locking drawers and cabinets, not leaving documents on desks unattended)
- not to remove personal data or devices containing or that can be used to access personal data from the Council's premises without prior authorisation and without adopting appropriate security measures (such as encryption or password protection) to secure the data and device
- 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 EEA except in compliance with the law and with the express authorisation from the Clerk or Chair of the Council
- to ask for help if unsure about data protection or if you notice a potential data breach or any areas of data protection or security that can be improved upon.

Failure to observe these requirements my amount to a disciplinary offence, which would be dealt with under the Council's disciplinary policy. 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 policy will be reviewed at least annually and updated as required.

Based on Model Data Protection Policy, NALC.