DATA PROTECTION POLICY

www.greathorkesley-pc.gov.uk

This Policy will be reviewed annually by Full Council.

Adopted: Full Council Meeting 6th February 2024 Minute Ref: 23/131 (b)

Reviewed:

PURPOSE

Great Horkesley Parish Council is committed to being transparent about how it collects and uses personal data, and to meeting data protection obligations. This policy sets out the council's commitment to data protection, and the 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 all personal data of current and former job applicants, current and former employees, contractors, members of the public and other personal data processed for council business. This policy applies to all data stored by the council, including on-premise, offsite and cloud services.

The procedures and principles set out herein must be always followed by the council, its employees, agents, contractors, councillors, or other parties working on behalf of the council. The council is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

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.

“The council” is Great Horkesley Parish Council.

DATA PROTECTION PRINCIPLES

The council processes personal data in accordance with the following principles, by:

- processing personal data lawfully, fairly and in a transparent manner in relation to the data subject.
- collecting personal data only for specified, explicit and legitimate purposes.
- processing personal data only where it is adequate, relevant, and limited to what is necessary for the purposes of processing.
- keeping accurate and up to date personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- keeping personal data for no longer than is necessary.
- adopting appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction, or damage.

The personal data that the council processes, the reasons for processing the data, how such data is used, how long such data is retained and the legal basis for processing it is stated in the council's privacy notices.

The council will not use a data subject's personal data for an unrelated purpose without telling them about it and the legal basis that the council intends to rely on for processing it. The council will not process personal data if it does not have a legal basis for processing it.

PROCESSING

The council will process personal data for one or more of the following reasons:

- The data subject has given consent to the processing of their personal data for one or more specific purposes.
- It is necessary for the performance of a contract or services, for example, a contract of employment.
- It is necessary to comply with any legal obligation.
- It is necessary for the council's vital or legitimate interests (or for the legitimate interests of a third party), unless there is a good reason to protect a data subject's personal data which overrides those legitimate interests.
- It is necessary to protect the vital or legitimate interests of the data subject or another person.
- 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 the council processes personal data in line with one of the above reasons, it does not require the consent of the data subject. Otherwise, the council is required to gain consent to process personal data. If the council asks for consent to process personal data, then they will explain the reason for the request. The data subject does not need to consent or can withdraw consent later.

Personal data may be held in secure files in hard copy and/or electronic format on IT systems and servers. The format of personal data, and periods for which the council holds personal data, are contained in the Data Retention Policy.

Sometimes the council will share personal data with contractors and agents to carry out obligations under a contract with the individual or for the council's legitimate interests. Those individuals or companies are required to keep personal data confidential and secure and to protect it in accordance with Data Protection law and the 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.

ROLES & RESPONSIBILITIES

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 the council's policies. They may have access to the personal data of other individuals and of members of the public in

the course of their work with the council. Where this is the case, the council relies on those working for, or on behalf of, the council to help meet the data protection obligations to staff and members of the public.

Individuals who have access to personal data are required:

- to access only data that they 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, and secure file storage and destruction including locking drawers and cabinets, and 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 the council's premises without prior authorisation and without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device.
- not to store personal data on local drives or on personal devices.
- to ask for help from the council's Data Protection Officer if they are unsure about data protection or if they 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 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.

Employees, councillors, and other data subjects are responsible for helping the council keep their personal data up to date. Data subjects should let the council know if data provided to the council changes, for example if they move to a new house or change bank details.

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

DATA BREACH NOTIFICATION PROCEDURES

The council have robust measures in place to minimise and prevent data breaches from occurring. Should a breach of personal data occur, the Clerk or Chairman of the council must be notified immediately, and the council must take notes and keep evidence of that breach.

If the council discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of a data subject (such as financial loss, breach of confidentiality, discrimination, or reputational damage), the Data Protection Officer must report it 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 Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without delay.

Data breach notifications shall include the categories and approximate number of data subjects and personal data records concerned, the name and contact details of the Data Protection Officer for the council, the likely consequences of the breach and details of the measures that will be taken by council to address the breach, including measures to mitigate its possible adverse effects.

DATA SECURITY

The council takes the security of personal data 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 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 our behalf, such parties do so based on written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

All data is kept and stored in line with the council's Data Retention Policy.

Procedures that are followed when processing personal data include:

- Transmitting personal data over secure networks only.
- Securely disposing of personal data that is to be erased. Hard copies are shredded, and electronic copies are deleted securely.
- Not sharing personal data informally. Any employee, councillor or other party working on behalf of the council that requires access to personal data should formally request such access.
- Storing all hard copies of personal data, along with any electronic copies stored on physical, removable media, securely, including the use of passwords where necessary.
- Handling all personal data with care, and not leaving it unattended or on view to unauthorised people at any time.
- Not retaining personal data on any device personally belonging to an employee or councillor, and only transferring personal data to devices belonging to agents, contractors or other parties working on behalf of the council where that party has agreed to comply fully with the spirit of this policy.

CONTACT INFORMATION

Great Horkesley Parish Council
Data Protection Officer (Parish Clerk)
parish-clerk@greathorkesley-pc.gov.uk

Information Commissioner's Office
https://ico.org.uk
0303 123 1113