

Hawkwell Parish Council

Data Protection Policy

Purpose

This Policy explains the duties and responsibilities of Hawkwell Parish Council and it identifies the means by which Council will meet its obligations.

Introduction

The General Data Protection Regulation (GDPR) which became law on 25th May 2018 and will, like the the Data Protection Act 1998 before it, seek to strike a balance between the rights of individuals and the Parish Council's legitimate reasons for using personal information. The Government have confirmed that despite the UK leaving the EU, GDPR will still be a legal requirement.

This Policy explains to the public, councillors and staff about GDPR.

Data Protection Terminology

Data subject - The person whose personal data is being processed. That may be: an employee; prospective or former employee, associate or prospective associate of HPC or someone transacting with it in some way; Member or volunteer, or persons transacting or contracting with one of our contractors/suppliers when we process data for them.

Personal data - Any information relating to a natural person or data subject that can be used directly or indirectly to identify the person. It can be anything from a name, a photo, and an address, date of birth, an email address, bank details, and posts on social networking sites or a computer IP address.

Sensitive personal data - Includes information about racial or ethnic origin, political opinions, and religious or other beliefs, trade union membership, medical information, sexual orientation, genetic and biometric data or information related to offences or alleged offences where it is used to uniquely identify an individual.

Data controller - A person who either alone, or jointly or in common with other persons (e.g. Parish Council, employer, council) determines the purposes for which and the manner in which any personal data is to be processed.

Data processor - In relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Processing information or data - Obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

- organising, adapting or altering it;
- retrieving, consulting or using the information or data;
- disclosing the information or data by transmission, dissemination or otherwise making it available;
- aligning, combining, blocking, erasing or destroying the information or data. regardless of the Technology used.

The policy is based on the premise that Personal Data must be:

- Processed fairly, lawfully and in a transparent manner in relation to the data subject.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date.
- Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- Processed in a manner that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Identifying the roles and minimising risk

GDPR requires that everyone within the Council must understand the implications of GDPR and that roles and duties must be assigned. The Council is the data controller and the Clerk is the primary data processor. The appointment of a Data Protection Officer (DPO) is not mandatory for councils under GDPR but it may be considered good practice to appoint an external DPO to avoid a conflict of interest.

Hawkwell Parish Council will adopt procedures and manage responsibly all data which it handles and will respect the confidentiality of both its own data and that belonging to partner organisations it works with, along with members of the public. In some cases, it will have contractual obligations towards confidential data, but in addition will have specific legal responsibilities for personal and sensitive information under data protection legislation.

The Council will be as transparent as possible about its operations and will work closely with public, community and voluntary organisations. Therefore, in the case of all information which is not personal or confidential, it will be prepared to make it available to partners and members of the Parish's communities. Details of information which is routinely available is contained in the Council's Publication Scheme which is based on the statutory model publication scheme for local councils.

GDPR requires continued care by everyone within the Council, councillors and staff, in the sharing of information about individuals, whether as a hard copy or electronically. A breach of the regulations could result in the Council facing a fine from the Information Commissioner's Office (ICO) for the breach itself and also to compensate the individual(s) who could be adversely affected. Therefore, the handling of information is seen as high/medium risk to the Council (both financially and reputationally) and one which must be included in the Risk Management Policy of the Council. Such risks can be minimised by undertaking an information audit, issuing privacy statements, maintaining privacy impact assessments (an audit of potential data protection risks with new projects), minimising who holds data protected information and the Council undertaking training in data protection awareness.

Processing of Personal Data

Council processes **personal data** in order to:

- fulfil its duties as an employer by complying with the terms of contracts of employment, safeguarding the employee and maintaining information required by law.
- pursue the legitimate interests of its business and its duties as a public body, by fulfilling contractual terms with other organisations, and maintaining information required by law.
- fulfil its duties in operating the business premises including security.
- assist regulatory and law enforcement agencies.

- process information including the recording and updating details about its councillors, employees, partners and volunteers.
- process information including the recording and updating details about individuals who contact it for information, or to access a service, or make a complaint.
- undertake surveys, censuses and questionnaires to fulfil the objectives and purposes of the Council.
- undertake research, audit and quality improvement work to fulfil its objects and purposes.
- carry out Council administration.

Where appropriate and governed by necessary safeguards Council will carry out the above processing jointly with other appropriate bodies from time to time.

The Council will ensure that at least one of the following conditions is met for personal data to be considered fairly processed:

- The individual has consented to the processing.
- Processing is necessary for the performance of a contract or agreement with the individual.
- Processing is required under a legal obligation.
- Processing is necessary to protect the vital interests of the individual.
- Processing is necessary to carry out public functions.
- Processing is necessary in order to pursue the legitimate interests of the data controller or third parties.

Protecting Confidential or Sensitive Information

Council recognises it must at times, keep and process sensitive and personal information about both employees and the public, it has therefore adopted this policy not only to meet its legal obligations but to ensure high standards.

Particular attention is paid to the processing of any **sensitive personal information** and the Parish Council will ensure that at least one of the following conditions is met:

- Explicit consent of the individual.
- Required by law to process the data for employment purposes.
- A requirement in order to protect the vital interests of the individual or another person.

Who is responsible for protecting a person's personal data?

The Parish Council as a corporate body has ultimate responsibility for ensuring compliance with the Data Protection legislation. The Council has delegated this responsibility day-to-day to the Parish Clerk.

- Email: info@hawkwellparishcouncil.gov.uk
- Phone: 01702 207710
- Correspondence: Hawkwell Parish Council, r/o Hawkwell Village Hall, Main Road, Hawkwell, Essex SS5 4EH

Complaints: If an individual has a complaint regarding the way their personal data has been processed, they may make a complaint to the Parish Clerk or the Information Commissioners Office

casework@ico.org.uk Tel: 0303 123 1113.

Information provided to us

The information provided (personal information such as name, address, email address, phone number) will be processed and stored so that it is possible for us to contact, respond to or conduct the transaction requested by the individual. By transacting with Hawkwell Parish Council, individuals are deemed to be giving consent for their personal data provided to be used and transferred in accordance with this policy, however wherever possible specific written consent will be sought. It is the responsibility of those individuals to ensure that the Parish Council is able to keep their personal data accurate and up-to-date. The personal information will be not shared or provided to any other third party or be used for any purpose other than that for which it was provided.

Data Security

The Parish Council cares to ensure the security of personal data. We make sure that your information is protected from unauthorised access, loss, manipulation, falsification, destruction or unauthorised disclosure. This is done through appropriate technical measures and appropriate policies. We will only keep your data for the purpose it was collected for and only for as long as is necessary, after which it will be deleted.

Appropriate technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. Personal data shall not be transferred to a country or territory outside the European Economic Areas unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Privacy Notices

Being transparent and providing accessible information to individuals about how Council uses personal data is a key element of GDPR. The most common way to provide this information is in a privacy notice. This is a notice to inform individuals about what a council does with their personal information. A privacy notice will contain the name and contact details of the data controller and, where appointed, the DPO, the purpose for which the information is to be used and the length of time for its use. It should be written clearly and should advise the individual that they can, at any time, withdraw their agreement for the use of this information. Issuing a privacy notice must be detailed on the Data Audit kept by Council. Council will adopt a privacy notice to use, although some changes could be needed depending on the situation, for example where children are involved. All privacy notices must be verifiable.

Children

Council will not process any data relating to a child (under 13) without the express parental/ guardian consent of the child concerned.

Data Audit

The data processor or DPO, where appointed, must undertake a data audit which details the personal data held, where it came from, the purpose for holding that data and with whom the Council share that data. This will include data held electronically or as a hard copy. Data held could change from year to year with different activities, and so the data audit will be reviewed at least annually or when the council undertakes a new activity.

Rights of a Data Subject (Individuals' Rights)

GDPR gives individuals rights with some enhancements to those rights already in place:

- the right to be informed
- the right of access
- the right of rectification
- the right to erasure
- the right to restrict processing
- right to data portability
- the right to object
- the right not to be subject to automated decision-making including profiling. *

*The Parish Council does not use automated decision making or profiling of individual personal data.

The two enhancements of GDPR are:

- (1) that individuals now have a right to have their personal data erased (sometimes known as the 'right to be forgotten' where their personal data is no longer necessary in relation to the purpose for which it was originally collected; and
- (2) data portability refers to the ability to move, copy or transfer data easily between different computers.

If a request is received to delete information, then the Data Processor (or DPO where appointed) must respond to this request within one month. If a request is considered to be manifestly unfounded then the request could be refused or a charge may apply. The charge will be as detailed in the council's Freedom of Information Publication Scheme. Council will be informed of such requests.

Data breaches

Any data breaches will be assigned to the Data Processor, or DPO if appointed, for investigation. Personal data breaches will be notified to Council and investigations must be undertaken within one month of the report of the breach. The ICO will be advised of a breach (within 3 days) where it is likely to result in a risk to the rights and freedoms of individuals.

It is unacceptable for employees, councillors and volunteers to use IT in any way that may cause problems for the Council, for example the discussion of internal Council matters on social media sites could result in reputational damage to the council and to individuals.

Summary

The main actions arising from this Policy are:

- The Council must be registered with the ICO.
- A copy of this policy will be available on the Council's website. The policy will be considered as a core policy for the Council.
- An information audit will be conducted and reviewed at least annually or when projects and services change or when further advice is issued by the ICO.
- Privacy notices must be issued.
- Data Protection will be included on Council's Risk Management Policy.

This policy document is written with current information and advice. All employees, councillors and volunteers are expected to comply with this policy at all times to protect privacy, confidentiality and the interests of the Council.