Helsington Parish Council Data Protection Policy

This policy was formally adopted by Helsington Parish Council (the Council) on 1 May 2013, and applies to all employees, and those acting on the Council's behalf.

Scope

An essential activity within the Council is the requirement to gather and process information about staff and people in the community in order to operate effectively. This will be done in accordance with the Data Protection Act 1998 (the Act), and other related government legislation.

The Council, acting as custodians of personal data, recognises its moral duty to ensure that all such data is handled properly and confidentially at all times, irrespective of whether it is held on paper or by electronic means. This covers the whole life cycle including:

- the obtaining of personal data;
- the storage and security of personal data;
- the use of personal data;
- the disposal / destruction of personal data.

The Council also has a responsibility to ensure that data subjects have appropriate access, upon written request, to details regarding personal information relating to them.

Actions

By following and maintaining strict safeguards and controls, the Council will:

A1. Acknowledge the rights of individuals to whom personal data relates, and ensure that these rights may be exercised in accordance with the Act;

A2. Ensure that both the collection and use of personal data is done fairly and lawfully;

A3. Ensure that personal data will only be obtained and processed for the purposes specified;

A4. Collect and process personal data on a “need to know” basis, ensuring that such data is fit for the purpose, is not excessive, and is disposed of at a time appropriate to its purpose;

A5. Ensure that adequate steps are taken to ensure the accuracy and currency of data;

A6. Ensure that for all personal data, appropriate security measures are taken, both technically and organisationally, to protect against damage, loss or abuse;

A7**.** Ensure that the movement of personal data is done in a lawful way, both inside and outside the Council and that suitable safeguards exist at all times.

Enablers

In order to support these actions, the Council will:

E1. Nominate a Data Protection Officer’ for the Council, responsible for gathering and disseminating information and issues relating to information security, the Act and other related legislation;

E2. Ensure that all activities that relate to the processing [1] of personal data have appropriate safeguards and controls in place to ensure information security and compliance with the Act;

E3. Ensure that all contracts and service level agreements between the Council and external third parties, where personal data is processed, make reference to the Act as appropriate;

E4. Ensure that those acting on the Council's behalf understand their responsibilities regarding information security under the Act, and that they receive the appropriate training / instruction and supervision so that they carry these duties out effectively and consistently and are given access to personal information that is appropriate to the duties they undertake;

E5. Ensure that all third parties acting on the Council's behalf are given access to personal information that is appropriate to the duties they undertake and no more;

E6. Ensure that any requests for access to personal data are handled courteously, promptly and appropriately, ensuring that either the data subject or his/her authorised representative has a legitimate right to access under the Act, that the request is valid, and that information provided is clear and unambiguous [2]

E7. Work towards adopting, as best working practice, the key principles of BS7799, the British Standard on Information Security Management;

E8. Review this policy and the safeguards and controls that relate to it at the Annual Meeting of the Council, to ensure that they are still relevant, efficient and effective.

---

[1] Processing as defined by the Act as obtaining, recording, holding, organisation, adaptation, alteration, retrieval, consultation, use, disclosure, alignment, combination, blocking, erasure and destruction.

[2] all actions regarding data subject access requests will be logged. This audit trail will include details regarding the nature of the request, the steps taken to validate it, the information provided as well as any withheld, e.g. for legal reasons.