



TOWN HALL
MARKET PLACE
HENLEY ON THAMES
RG9 2AQ

www.henleytowncouncil.gov.uk

TEL: 01491 576982

FAX: 01491 571660

DATA PROTECTION AND RETENTION POLICY

1. PURPOSE AND SCOPE

- 1.1 The 1998 Data Protection Act came into force from 1 March 2000. Henley Town Council supports the objectives of the Act and will comply with it.
- 1.2 The purpose of this Policy Statement is to formalise the position of the Council and state its commitment to maintaining confidentiality of personal information within its record systems. Records include electronic records.
- 1.3 This Policy Statement also ensures that necessary records and documents are adequately protected and maintained and ensures that records which are no longer needed or are of no value are discarded at the appropriate time. This policy relates to electronic records as well as physical hard copies.

2. BACKGROUND

- 2.1 Henley Town Council recognises that it must, at times, keep and process sensitive and personal information concerning employees, Councillors and the public. It has adopted this policy to meet its legal obligation under the Data Protection Act 1998 and to ensure high standards of practice under the Lord Chancellor's Code of Practice on the Management of Records issued under Section 46 of the Freedom of Information Act 2000 which applies to public authorities. The Council is open about its operations and works closely with the community. In the case of information that is not personal or confidential the Town Council is prepared to make information available to the public. Information which is available is indicated in the Council's 'Freedom of Information' page on the website.
- 2.2 The Data Protection Act 1998 (the Act) regulates the holding and processing of personal data – ie information relating to living individuals, which is held either on a computer, a server, a secure website, or in some cases in manual form. The Act also gives rights

to individuals whose personal information is held by organisations.

- 2.3 The Council needs to collect and use personal information in order to carry out its functions effectively. Information can be held concerning its current, past and prospective employees, suppliers, service users, residents and others with whom the Council communicates.
- 2.4 The Council and in some cases its individual employees could face prosecution for failure to handle personal data in accordance with the Act.

3. POLICY STATEMENT

- 3.1 Any personal data which the Council collects, records or uses in any way whether it is held on paper, computer or other media will be subject to appropriate safeguards to ensure that the Council complies with the Act.
- 3.2 The Council endorses and adheres to the following Principles which are set out in the Act regarding personal data, which shall be:
 - a) Fairly and lawfully processed
 - b) Be processed for specific and lawful purposes only;
 - c) Adequate, relevant and not excessive;
 - d) Accurate and kept up to date;
 - e) Not kept for longer than is necessary – see appendix 1 for further information;
 - f) Processed in line with the data subject's rights
 - g) Protected appropriately against authorised or unlawful processing and accidental loss or destruction;
 - h) Kept secure and not transferred to a country that does not have adequate data protection laws.

4. ACTION

- 4.1 In order to meet the requirements of the data protection principles and its obligations under the Act, the Council will ensure the following:
 - 4.1.1 Renew its entry of the Register of Notifications held by the Information Commissioner's Office.
 - 4.1.2 Ensure officers have specific responsibility for data protection in the Council.
 - 4.1.3 Any forms used to collect data will contain a 'fair processing notice' to inform the data subject of the reasons for collecting the personal information and the intended uses.

- 4.1.4 Any personal information that has been collected will be used only for the purposes for which it was collected.
- 4.1.5 Data subjects (individuals to whom the personal information relates) are able to exercise their rights under the Act, including:
- the right to be informed that their personal information is being processed
 - the right of access to their personal information
 - the right to correct, rectify, block or erase information that is regarded as wrong
- 4.1.6 Personal data will only be disclosed to third parties when it is fair and lawful to do so in accordance with the Act and with any Information Sharing Protocols.
- 4.1.7 Sensitive personal data will only be processed with the explicit consent of the data subject or if an exemption applies under the Act. Sensitive data is personal data about an individual's racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sex life, details of the commission or alleged commission of any offence and any court proceedings relating to the commission of an offence.
- 4.1.8 Procedures are in place to check the accuracy of personal data collected, retained and disclosed.
- 4.1.9 Review the time that personal information is retained or stored to ensure that it is erased at the appropriate time.
- 4.1.10 When a Subject Access Request (SAR) is received, the Council has 40 calendar days in which to respond and a maximum fee of up to £10 can be charged for the information requested. Payment needs to be made in full before the information will be provided and the 40 calendar days rule becomes effective from this date. There are exceptions when the request for information may be refused as detailed within the new ICO guidance notes.
- 4.1.11 All officers who hold or process personal information will receive appropriate training in order to comply with the Act.
- 4.1.12 Audit compliance with this policy and the Act and any incidents involving breaches of this policy and the Act are recorded, analysed and disciplinary action taken as appropriate.
- 4.1.13 This policy is reviewed regularly and updated when necessary.

Prepared: December 2016

Approved: January 2017